موسسه فرهنگی مطالعات
وتحقیقات بین المللی ابرار معاصر تهران

چاپ سوم

جنگ نرم ۳

نبرد در عصر اطلاعات

جنگ نرم (۳)
(نبرد در عصر اطلاعات)

مؤسسهٔ فرهنگی مطالعات و تحقیقات
بین‌المللی ابرار معاصر تهران

۱۳۸۶

سرشناسه	: عبدالله‌خانی، علی، ۱۳۴۳ -
عنوان و پدیدآور	: جنگ نرم (۳): (نبرد در عصر اطلاعات)/ گردآوری و تدوین دکتر علی‌عبدالله‌خانی.
مشخصات نشر	: تهران: مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران، ۱۳۸۹.
مشخصات ظاهری	: ۲۹۸ ص.: جدول، نمودار.
فروست	: انتشارات مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران؛ ۲۶۹.
شابک	: ۶۰۰۰۰ ریال: 978-964-526-132-8
وضعیت فهرست‌نویسی	: فیپا.
یادداشت	: کتابنامه.
موضوع	: جنگ اطلاعاتی.
شناسه افزوده	: مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران.
رده‌بندی کنگره	: ۱۳۸۶ ۹ ج ۲ ع/ ۱۶۳ U
رده‌بندی دیویی	: ۳۵۵/۳۴۳
شماره کتابشناسی ملی	: ۱۱۸۹۴۲۷



انتشارات مؤسسهٔ فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران

تهران: صندوق پستی ۳۸۴۹ـ ۱۵۸۷۵، تلفن: ۸۸۵۰۰۲۵۰، نمابر: ۸۸۷۵۶۲۰۷

نشانی اینترنت:www.tisri.org پست الکترونیک: info@tisri.org

جنگ نرم (۳) (نبرد در عصر اطلاعات)

نظارت و اجرا: مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران ـ معاونت پژوهشی

گردآوری و تدوین: علی عبدالله‌خانی

صفحه‌آرا: منصوره سعادت

ویراستار: منیره آذری

حروفچین: زهره اسماعیل‌زاده

نمونه‌خوان: ساقی پناهی‌نژاد

طراح جلد: مریم جعفری نائینی

چاپ نخست: اسفندماه ۱۳۸۶

چاپ دوم: اسفندماه ۱۳۸۷

چاپ سوم: دی ماه ۱۳۸۹

شابک: ۸ ـ ۱۳۲ ـ۵۲۶ ـ ۹۶۴ ـ ۹۷۸

کدبازیابی در کتابخانه دیجیتالی دید: BB00020085103060511

چاپ و صحافی: باقری

شمارگان: ۱۰۰۰ نسخه

قیمت: ۶۰۰۰ تومان

پیش‌گفتار ناشر

نقش اطلاعات در حوزه‌های استراتژیک و امنیتی همواره ارزنده و ذی‌نفوذ بوده است. اما این نقش از اواخر قرن بیستم دچار تغییر و تحولات بنیادین گشت تا جایی‌که اطلاعات به یک متغیر مستقل و یکی از کانون‌های اصلی حوزه‌های استراتژیک و امنیت تبدیل گردید.

کتاب جنگ نرم (۳) ویژه نبرد در عصر اطلاعات در چارچوب سلسله کتاب‌های جنگ نرم به منظور آشنایی هرچه بیشتر خوانندگان نسبت به نقش و تأثیر اطلاعات به عنوان مجرا و محتوا در نبردهای آینده تنظیم گشته است. این کتاب در کنار دو شماره گذشته و یک شماره بعدی (شماره ۴) سلسله کتاب‌های جنگ نرم، مجموعه‌ای نسبتاً کامل از بررسی و مطالعه اطلاعات در نبردهای آینده است.

امید است کتاب جنگ نرم (۳) بتواند به درک هرچه بیشتر خوانندگان خصوصاً استراتژیست‌ها از نقش اطلاعات در نبردهای آینده کمک نماید.

مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی

ابرار معاصر تهران

معاونت پژوهشی

فهرست

مقدمه

نبرد اطلاعاتی، مفهوم جدیدی نیست، بلکه پدیده «موج سوم» و محصول فرعی انقلاب رایانه است؛ در واقع، حتی به نوع بشر نیز اختصاص ندارد. فاخته را در نظر بگیرید! این رزمنده نبرد اطلاعاتی با تخم گذاشتن در آشیانه پرندگان دیگر، تا ۱۸۰ گونه از پرندگان را چنان فریفته است که آنان پدر و مادر «رضاعی» او می‌شوند. برای فریفتن پرنده صاحب آشیانه، فاخته تخم خود را به شکل تخم میزبان درمی‌آورد و با این رفتار خود، تمامیت محیط اطلاعاتی میزبان را از بین می‌برد. دیگر، شکل ظاهری تخم، منبع قابل اعتماد اطلاعات نیست. در مثالی دیگر، زغن ژست‌های خاضعانه مصنوعی به‌خود می‌گیرد تا رقبای مورد تنفرش را به جلو بکشاند و وقتی رقیب پیش آمد، به حمله‌ای ناگهانی مبادرت می‌کند. در این مورد نیز زغن تمامیت محیط اطلاعات رقیب را از بین برده است. نباتات و حیوانات جهت محافظت از اطلاعاتی که برای بقای آنها جنبه حیاتی دارد نیز از روش‌های نبرد اطلاعاتی دفاعی استفاده می‌کنند؛ مثلاً ممکن است برای اینکه گونه‌هایی که در زنجیره غذایی بالاتر از آنها هستند متوجه‌شان نشوند، در سایه قرار بگیرند یا به رنگ‌های مخصوص درآیند.[1]

انسان همواره سعی کرده است از اطلاعات ارزشمند خود در برابر رقیب محافظت کند. حدود پنج هزار سال پیش، امپراتوران چین راز تولید ابریشم را حفظ می‌کردند؛ اینکه کرم

---

1. Lôyal Rue, By the Grace of Guile: The Role of Deception in Natural History and Human Affairs, New York: Oxford University Press, 1994, pp. 120-122.

به‌خصوصی این الیاف را تولید می‌کند، درخت‌های توت که منبع غذا و محل سکونت این کرم‌ها هستند و فن بافتن که این الیاف را به پارچه‌های عالی تبدیل می‌کند، رازهایی بودند که باید حفظ می‌شدند و برای فاش کردن آن، مجازات مرگ با شکنجه مقرر شده بود. سیستم امنیتی آنها حدود سه هزار سال عمل کرد تا اینکه شاهزاده خانمی که برای ازدواج با شاهزاده‌ای به سرزمینی دور رفته بود، این راز را فاش ساخت. در سال ۱۵۰۰ قبل از میلاد، حکاکی اهل بین‌النهرین، از راز براق کردن سفال با روشی مطمئن‌تر محافظت نمود. او دستورالعمل این کار را با خط میخی روی لوحی که از گل رس بود با عبارات رمزی نوشت. در قرن اول قبل از میلاد، ژولیوس سزار از ترس اینکه پیام‌هایش خوانده شود، نامه‌های خود را به سیسرون و دوستان دیگر با علائم رمزی که امروزه به نام او خوانده می‌شود نوشت.[1]

نمونه‌های نبرد اطلاعاتی را می‌توان در سرتاسر تاریخ بشر پیدا کرد. حدود ۱۲۰۰ سال قبل از میلاد، یونانیان با ازبین بردن تمامیت سیستم‌های بصری مورد استفاده تروایی‌ها وارد تروا شدند. چه کسی فکر می‌کرد که یک اسب چوبی، استتارکننده ارتش کوچکی از سربازان باشد؟ در قرون دوازده و چهارده، مغولان موفق شدند با پی‌بردن به محل دقیق استقرار دشمنان و مخفی‌گاه داشتن محل‌های خود، ارتش‌های بزرگ امپراطوری چین و مسیحیت را منهدم کنند. در نبرد لایگنیتز[2] به سال ۱۲۴۱ میلادی، مغولان نیروهای ائتلاف لهستان ـ پروس را که تعدادشان چهار برابر آن‌ها بود شکست دادند. مغولان با اطلاع از نظم جنگی نیروهای ائتلاف، آن‌ها را فریب دادند که به تعقیب دسته‌های کوچک بپردازند و در نتیجه، این دسته‌ها تعقیب‌کنندگان را به چنگال نیروهای اصلی مغول گرفتار کردند. در ناپلئونی، نیروی دریایی سلطنتی بریتانیا ارتباطات استراتژیک دریایی نیروهای اعزامی ناپلئون به شمال آفریقا را قطع کرد و این موجب شکست ناپلئون شد.[3]

1. Ibid
2. Liegnitz
3. **Risky Business: The Threat from Economic Espionage,** video, The National Counterintelligence Center, 1997.

با اینکه نبرد اطلاعاتی مقوله جدیدی نیست، می‌توان گفت با فناوری‌ها و رسانه‌های اطلاعاتی جدید دستخوش تحول شده است. در آغاز قرن بیستم، یک رزمنده نبرد اطلاعاتی، برای دزدیدن اسرار به سیستم رایانه دستبرد نمی‌زد، ویروس رایانه‌ای مخرب وارد شبکه نمی‌کرد، مکالمات تلفن همراه را گوش نمی‌داد، با ماهواره‌های جاسوسی تصویربرداری نمی‌کرد. یا از ایستگاه‌های رادیویی و تلویزیونی، تبلیغات و اطلاعات غلط پخش نمی‌کرد. البته این فناوری‌ها هم وجود نداشت. تا سال ۱۹۵۰ رایانه، رادیو و تلویزیون اختراع شده بود؛ اما در اختیار کمتر کسی قرار داشت و هیچ‌کدام از آنها نیز به‌هم متصل یا حتی از راه دور قابل دسترسی نبودند. وب سایتی وجود نداشت که به آن دستبرد زده شود. اینترنتی وجود نداشت که مورد استفاده قرار گیرد و با سایت‌های اینترنتی معامله‌ای انجام نمی‌شد که بتوان به آنها پی برد. هیچ پیام پست الکترونیکی (ایمیل) وجود نداشت که بتواند حاوی رمز زیانباری باشد.[1] روش کم‌هزینه‌ای که با آن، فرد معمولی بتواند به‌طور بالقوه به میلیون‌ها نفر ویروس‌های مخرب رایانه‌ای، پیام‌های تنفر، نظریه‌های توطئه‌آمیز و وحشت انتقال دهد، موجود نبود.[2]

در دهه شصت، رایانه‌ها به‌هم متصل شدند. این کار، ابتدا در داخل سازمان‌ها به‌صورت شبکه‌های محلی انجام گرفت. تا سال ۱۹۶۹ اولین شبکه وسیع در داخل ایالات متحده عمل می‌کرد. این شبکه که به نام حامی آن، یعنی آژانس پروژه پژوهش پیشرفته وزارت دفاع[3]، آرپانت[4] نامیده شده بود، مؤسسه پژوهشی استانفورد دانشگاه کالیفرنیا واقع در لوس‌آنجلس، دانشگاه کالیفرنیا واقع در سانتاباربارا و دانشگاه یوتا را به‌هم متصل می‌کرد. این شبکه تکامل یافت و اینترنت شد (شبکه شبکه‌ها که جهان را دربرمی‌گیرد). در سال ۱۹۹۰ که سرانجام مأموریت آرپانت به پایان رسید، اینترنت بیش از سیصد هزار میزبان داشت. این تعداد در سال ۱۹۹۲ به یک میلیون، در سال ۱۹۹۶ به ده میلیون و تا سال ۱۹۹۸ به ۳۰ میلیون نفر رسید. در

1. David Kahn, **The Codebreakers,** New York: Macmillan, 1967, p. 75.
2. Ibid., pp. 83-84.
3. The Department of Defense Advanced Research Project Agency
4. ARPANET

سپتامبر ۱۹۹۸ شرکت ایرلندی NUA برآورد کرد که در سرتاسر جهان ۱۴۷ میلیون نفر از اینترنت استفاده می‌کنند.[1] این رقم در سال ۲۰۰۴ به بیش از ۵۰۰ میلیون نفر رسیده است.

نیکلاس نگروپونت[2]، مؤسس و مدیر آزمایشگاه رسانه‌ها در مؤسسه تکنولوژی ماساچوست پیش‌بینی کرد که تا سال ۲۰۰۸ تعداد کسانی که از اینترنت استفاده خواهند کرد به یک‌میلیارد نفر خواهد رسید که بیشتر آنها به کشورهای درحال توسعه تعلق خواهند داشت. پیش‌بینی او بیشتر به برنامه‌های گسترش ماهواره‌ای مدار ـ زمین ایستگاه زمینی ثابت[3] و ماهواره‌های مدار ـ زمین کم‌ارتفاع[4] در مدار زمین استوار است. SGEO و SLEO در پهنای باند بالا و با هزینه کم، ایستگاه‌های ثابت و متحرک را چه در نواحی پرجمعیت شهری کشورهای توسعه‌یافته قرار داشته باشند و چه در نواحی روستایی کشورهای در حال توسعه به‌هم متصل خواهد کرد. سیستم ایریدیم[5] که در نوامبر ۱۹۹۸ کار خود را آغاز کرد، ۶۶ ماهواره LEO (به‌اضافه ماهواره‌های یدکی) دارد که دور زمین می‌گردند. وقتی کل افراد آنلاین در جهان افزایش یابد، تعداد بازیگران بالقوه نبرد اطلاعاتی تهاجمی و اهداف حمله به آنها نیز بیشتر خواهد شد.[6]

در حال حاضر رایانه در همه‌جا وجود دارد. رایانه‌ها ارزان، اغلب کوچک و به‌هم مرتبط هستند و در همه‌چیز، از مایکروفرها تا موشک‌های هدایت‌شونده دقیق تعبیه شده‌اند. رایانه در تمام انواع فرایندها ازجمله: فرایندهای تجاری، بانکداری و مالیه، حمل‌ونقل و دریانوردی، انتقال آب و انرژی، آموزش‌وپرورش، تفریحات، دولت، مراقبت‌های بهداشتی، خدمات اورژانس و عملیات نظامی مورد استفاده قرار می‌گیرد. رایانه‌ها تجارت الکترونیکی، پزشکی، کنفرانس و ارتباط از راه دور را ممکن کرده‌اند. یکی از پیامدهای این تحول آن است که اطلاعات حساسی که زمانی محدود به گفت‌وگوهای درون ادارات و اسناد کاغذی بود، اکنون

---

1. John Arquilla and David Ronfeldt, "Cyberwar Is Coming"! **Comparative Strategy**, Vol. 12, 1993, pp. 141-165.
2. Nicholas Negroponte
3. Geostationary Earth-Orbiting Satellites (SGEO)
4. Low-Earth-Orbiting Satellite (SLEO)
5. Iridium
6. Ibid.

رایانه‌ای شده، به‌وسیله شبکه‌های عمومی انتقال داده می‌شود و درنتیجه به‌طور بالقوه در معرض سرقت، بهره‌برداری و خرابکاری از راه دور قرار می‌گیرند.[1]

پیشرفت رایانه با پیشرفت مشابهی در حسگرها همراه بوده است. این حسگرها راه را برای آینده که اطلاعات به آسانی در اختیار افراد دوردست باشد هموار می‌کنند.

رایانه‌ها با حسگرها و سایر فناوری‌های اطلاعاتی، برای ما خانه، اتومبیل و دفاتر هوشمند به‌همراه می‌آورند. خانه فناوری بالای[2] بیل گیتس، به نام زانادو ۲/۰، نسیم نگاهی به آینده را ممکن می‌سازد. ساکنان این خانه، سنجاق‌های کوچکی به لباس‌های خود زده‌اند که به رایانه امکان می‌دهد به محل آنها پی ببرد و محیط را به‌نحو دلخواهشان تنظیم کند. وقتی آنها در خانه حرکت کنند، تلویزیون‌هایی که به‌دقت تنظیم شده‌اند، آثار هنری انتخابی آنها را پخش می‌کنند و موسیقی، نور و شرایط محیطی مطابق دلخواه آنهاست. اگر آنها یک فیلم یا برنامه تلویزیونی را انتخاب کنند، نزدیک‌ترین صفحه تلویزیون، آن را نمایش می‌دهد. اگر به رایانه گفته باشند که به آنها تلفن خواهد شد، فقط نزدیک‌ترین گوشی زنگ می‌زند. اگر خانه‌های ما به اینترنت وصل شده باشد، آیا غریبه‌ها خواهند توانست وسایل خانگی‌مان را خاموش و روشن کنند یا به حرف‌های خصوصی ما گوش بدهند؟ آیا قادر خواهند بود سیستم امنیت خانه را از کار بیندازند؟[3]

اینترنت بر مجموعه‌ای از پروتکل‌های قلمرو عمومی مانند: پروتکل کنترل مخابره[4] و پروتکل اینترنت[5] مبتنی است. این پروتکل‌ها، قواعدی را که با آنها رایانه‌ای با رایانه دیگر گفت‌وگو می‌کند و چگونگی مسیریابی پیام‌ها را مشخص می‌کنند. سوئیت پروتکل TCP یا IP

1. For a Brief history of the Internet, See Peter J. Denning, "The Internet after Thirty Years," in Dorothy E. Denning and Peter J. Denning, eds., **Internet Besieged: Countering Cyberspace Scofflaws,** Addison-Wesley, ACM Press, 1997, pp. 15-27.
2. High Technology
3. Nicholas Negroponte, "The Third Shall Be First", **Wired News,** Vol. 6, No. 1, Jan. 1998, p. 96.
4. Transmission Control Protocol (TCP)
5. Internet Protocol (IP)

اکنون در شبکه‌های داخلی شرکت‌ها (اینترانت‌ها) و شبکه‌های خارجی آنها (اکسترانت‌ها) به فراوانی استفاده می‌شود. اکسترانت‌ها تأسیسات مختلف یک شرکت را به‌هم متصل و اتصال با مشتریان، شرکا و تهیه‌کنندگان مواد مورد نیاز شرکت را برقرار می‌کنند.[1] استفاده از این پروتکل‌های استاندارد، عملیات متقابل در سرتاسر شبکه را ممکن می‌سازد. درحالی‌که این پروتکل‌ها، امکان ارتباط و سهیم بودن تأسیسات را فراهم می‌کنند، اشکالاتی نیز دارند. در سازمان‌ها و سکوهای رایانه‌ای، درجه آسیب‌پذیری بالا می‌رود و ممکن است با یک حمله، هزاران سیستم از بین بروند. قابلیت بین‌عملیاتی[2] موجب همگرایی شبکه‌ها و درنتیجه به‌هم مربوط شدن فرایندهای امور داخلی و خارجی (از موجودی انبار و حمل‌ونقل تا فروش و بازاریابی) می‌شود.

ممکن است روزی فرا برسد که در عمل، تمام دستگاه‌ها و فرایندها به این شبکه جهانی متصل شده باشند. چنین پدیده‌ای بر نبرد اطلاعاتی، اثر عمیقی خواهد داشت. آیا متجاوز الکترونیکی خواهد توانست سیستم امنیت یک فرودگاه را برهم زند یا درهای یک مجتمع نظامی را باز کند؟ آیا آنها خواهند توانست موجب شوند اتومبیلی که با سرعت هفتاد مایل در ساعت در اتوبان حرکت می‌کند خراب شود، صد اتومبیل به‌هم بخورند، یا مسیر ترافیک عوض شود؟ آیا متجاوزان، دزدان و ضاربان قادر خواهند بود در سایت‌هایی که تصاویر اماکن عمومی یا داخل منازل را نشان می‌دهند، حرکات قربانیان خود را دنبال کنند؟[3]

فناوری‌های اطلاعات به‌صورت کارت‌های کوچکی که حاوی اطلاعات شخصی ما و وسایل ارتباطی برای برقراری ارتباط تلفنی، پیج کردن و خدمات پست الکترونیکی خواهند بود و ابزارهای آن به شنوایی و سایر اعمال بدن کمک خواهند کرد، به‌طور فزاینده‌ای به بدن ما متصل خواهند شد. در کارخانه مونتاژ هواپیمای بوئینگ واقع در اورت[4] واشنگتن، در حال

---

1. Jennifer Lenhart, "Keeping an Electronic Eye on the Kids," **Washington Post,** May 29, 1998.
2. Interoperability 3. Frex
3. Richard Folkers, "Xanadu 2.0," **U.S. News & World Report,** Dec. 1, 1997, p. 87.
4. Everett

آزمایش لباس‌های واقعی‌ای هستند که در عمل مورد استفاده آنهاست.[1] در قسمت کمر این لباس‌ها، رایانه‌ای شخصی با برنامه ویندوز نصب می‌شود. این کارگران کلاهی بر سر می‌کنند که دارای سخت‌افزار تعیین وضعیت است و یک صفحه نمایش دارد. این مجموعه دارای یک دست الکترونیکی راهنما نیز هست که کارگران را از کنترل مستمر نمودارهای روی کاغذ و فهرست قطعات بی‌نیاز می‌کند. یک شرکت وابسته به سونی به فروش رایانه‌های پرقدرت قابل پوشیدن به نام یاور سیار[2] مبادرت نموده است. این رایانه دو پوندی می‌تواند با صدا فعال شود و با صفحه نمایشی که به سر گذاشته می‌شود مورد استفاده قرار گیرد. کاربران آن قادر خواهند بود تلفن کنند، دورنگار بفرستند و به اینترنت وصل شوند. اگر فرد خرابکاری وارد یکی از این سیستم‌ها شود و مثلاً صفحه نمایش را تغییر دهد، چه اثری بر کسی که آن رایانه را «پوشیده است» خواهد داشت؟[3]

روزی ممکن است نوعی تراشه (چیپ) رایانه‌ای را ببینیم که به‌طور مستقیم با سلول‌های مغز کار می‌کنند. این تراشه‌ها قادر خواهند بود برای کمک به نابینایان دوربین‌های کوچکی به مغز متصل کنند یا برای تقویت حافظه ما و سایر فعالیت‌های مغز به‌کار روند. پژوهشگران مؤسسه فناوری کالیفرنیا در حال آزمایش تراشه‌های سیلیکون هستند که با استفاده از تکنیک‌های مدار یکپارچه (مدار انتگره) استاندارد ساخته شده‌اند.[4] این تراشه‌ها دارای شانزده گودی هستند و هر یک از آنها به اندازه یک تار موی انسان قطر دارد. این گودی‌ها با مواد تغذیه‌کننده عصب و سلول‌های عصبی مغز جنین موش پر شده‌اند. از این سلول‌ها، نرون‌هایی رشد می‌کنند که خود را به دیواره‌های جداکننده گودی‌ها می‌رسانند و همانند آنچه در یک مغز در حال گسترش روی می‌دهد، به یکدیگر مرتبط می‌شوند. آتشبازی بین سلول‌های عصبی که

---

1. **Business Wire,** New York, January 16, 1997.
2. Mobile Assistant
3. Christopher Elliott, "Everything Wired Must Converge", **Journal of Business Strategy,** Dec. 31, 1997.
4. Jim Nash, "Wiring the Jet Set", **Wired News,** Oct. 1997, pp. 129.

شبیه مسیرهای برقی اثرگذار بر حافظه در مغز است، به‌وسیله الکترودهای کوچکی که به گودی‌ها وصل شده‌اند کشف می‌شود.[1] الکترودها، رایانه‌ای را که عوامل مؤثر بر ارتباطات نرون‌ها را تجزیه و تحلیل می‌کند تغذیه می‌کنند.[2] پژوهشگران اظهار می‌دارند که این تراشه‌ها سرانجام قادر خواهند شد فعالیت‌های مختلف مغز را تقویت کنند.[3] یک تراشه مغز را مجسم کنید که ازطریق ارتباط بدون سیم به اینترنت وصل شده و به ما اجازه می‌دهد مردم و محل‌های طرف دیگر سیاره را ببینیم، با صدا و پست الکترونیکی با دیگران ارتباط برقرار کنیم و به اطلاعات موجود در شبکه‌ها دسترسی آسان داشته باشیم. نبرد اطلاعاتی در تمام ابعاد جدید خود خواهد بود، نه در آنچه ما برایش آمادگی داریم. آلوده کردن رایانه شخصی ما با ویروس یک مسئله است و ویروسی کردن رایانه‌ای که مغز ما را تغذیه می‌کند مسئله‌ای دیگر. تراشه‌های مغز به‌طور بالقوه حتی قادرند اشکال جدیدی از عملیات روانشناختی به‌وجود آورند.[4]

زیرساخت‌های حساس یک کشور، ازطریق اتوماسیون و قابلیت اتصال، به‌طور فزاینده به یکدیگر وابسته می‌شوند؛ مثلاً سیستم‌های مخابرات و رایانه‌ها، از توزیع انرژی، خدمات اضطراری، حمل‌ونقل و خدمات مالی پشتیبانی می‌کنند. بیش از ۹۵ درصد مخابرات نظامی از خط پیوندهای (لینک‌های) غیرنظامی می‌گذرد. بنابراین، حمله‌ای با این ماهیت علاوه‌بر فعالیت‌های غیرنظامی، کل عملیات نظامی را تحت تأثیر قرار خواهد داد.[5]

با توجه به ابعاد، گستره و زوایای نبرد اطلاعات و تبدیل شدن اطلاعات به پدیده‌ای فوق‌العاده به‌عنوان محتوا و برای عمل، شناخت هرچه بیشتر آن سودمند و ضروری است. این

---

1. "Xybernaut Plans Wearable PC", **Reuters, special to CNET News,** May 15, 1998.
2. Rick Weiss, "Neurology: Computer Chips for the Brain", **Washington Post,** Oct. 27, 1997, p. A2.
3. Donn B. Parker, "Automated Crime," in **Cybercrime,** International Conference Course Book, Oceana Publications, Washington, DC, Oct. 30-31, 1997, and New York, Nov. 17-18, 1997.
4. David G. Boney, "The Plague: An Army of Software Agents for Information Warfare", **paper for CS 229, George Washington University,** Dec. 11, 1997.
5. John Petersen, "Information Warfare: The Future", in Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, eds., **Cyberwar: Security, Strategy and Conflict in the Information Age,** AFCEA International Press, Fairfax, VA, 1996, pp. 219-226.

کتاب قصد دارد تا جنبه‌های امنیتی نبرد اطلاعات را مورد بررسی قرار دهد. به‌همین‌منظور اغلب از مقالات یا نوشته‌های قوی و سودمندی که در نقاط مختلف جهان نگاشته شده، بهره‌مند گردیده است.

کتاب «نبرد در عصر اطلاعات» دارای هشت فصل است. در فصل اول تأثیر تکنولوژی اطلاعات بر امنیت ملی مورد بررسی قرار خواهد گرفت و دراین‌خصوص نقش و تأثیر اطلاعات بر تحول مفهومی و مدیریت امنیتی مورد توجه است.

در فصل دوم تلاش خواهد شد تا معانی، مؤلفه‌ها و اجزای نبرد اطلاعات به‌عنوان حوزه مطالعاتی مورد بررسی قرار گیرد. در این فصل تمایزات میان نبرد به‌عنوان محتوا و نبرد به‌عنوان مجرای انتقال اطلاعات مورد توجه قرار خواهد گرفت؛ علاوه‌برآنکه درباره این مفهوم در عرصه‌های ذهنی و فیزیکی به‌عنوان دو بعد اصلی بحث خواهد گردید.

فصل سوم تحت عنوان «استراتژی‌ها و تاکتیک‌های نبرد اطلاعات» از بخش‌های مهم این کتاب است که توسط دو تن از کارشناسان ارشد حوزه مطالعاتی نبرد اطلاعاتی پرتال‌های مت‌بیشاب و امیلی گلدمن نگاشته شده است. این مقاله با ترسیم محیط منازعه، انواع نبرد اطلاعاتی را به چهار بخش اساسی تقسیم می‌نماید که در آن نبرد غیرکشنده اصلی‌ترین و ناب‌ترین نوع نبرد اطلاعاتی تلقی شده است.

فصل چهارم اشکال و ابزار جنگ اطلاعات را مورد بحث و بررسی قرار داده است. دراین‌چارچوب جنگ C4I، جنگ مبتنی‌بر اطلاعات ـ عملیات، جنگ الکترونیکی، جنگ ادراکی و جنگ سایبر به‌عنوان مهم‌ترین و اصلی‌ترین اشکال نبرد اطلاعات بحث گردیده است. همچنین سلاح‌های HERF و فرستنده پالس الکترومغناطیسی ازجمله مهم‌ترین سلاح‌های جنگ اطلاعاتی مورد توجه و بررسی قرار گرفته است.

فصل ششم به‌طور کامل و مبسوط تکنولوژی‌های حفاظت در نبرد اطلاعات را بررسی نموده است. در این فصل رمزی‌سازی، سری‌نگاری، گمنام‌سازی، بهداشتی کردن، دفع آشغال، سپرسازی و قفل‌ها و کلیدهای حفاظتی ازجمله مهم‌ترین تکنولوژی‌های حفاظت در نبرد

اطلاعاتی معرفی و مورد بحث قرار گرفته‌اند.

فصل هفتم یکی از جنبه‌های مهم نبرد اطلاعاتی، یعنی نبرد الکترونیکی را مورد بررسی قرار داده است. هدف اصلی این فصل آشناسازی خوانندگان با جنبه‌ها، ابعاد و کارکردهای مهم جنگ الکترونیک است.

فناوری‌های زیست‌سنجی عنوان فصل هشتم این کتاب است. در این فصل انواع مختلف و نوین فناوری‌های زیست‌سنجی به‌ویژه فناوری عنبیه چشم، شکل دست‌ها، شناسایی صورت، تشخیص صدا و شناسایی ازطریق DNA مورد بررسی قرار گرفته است.

در فصل هشتم مسئله حفاظت از زیرساخت‌های حیاتی اطلاعاتی بررسی شده است. در این فصل ابتدا مفهوم و انواع زیرساخت‌های جهانی مشخص شده و سپس درخصوص مدل‌های مختلف حفاظت از زیرساخت‌های حیاتی اطلاعاتی در کشورهای مختلف بحث گردیده است.

والسلام

علی عبداله‌خانی

۸۶/۱۲/۸

فصل اول
امنیت در عصر تکنولوژی اطلاعات

- درآمد
- مدیریت درگیری‌ها در عصر اطلاعات
- سازماندهی و هدایت جنگ در عصر اطلاعات
- حاکمیت در عصر اطلاعات

۱. درآمد

تسلیحات هدایت‌شوندهٔ دارای سیستم GPS (سیستم موقعیت‌یاب جهانی)، ارتش‌های مدرن را قادر ساخته‌اند تا در شب یا شرایط جوی نامناسب، هدف‌گیری دقیقی داشته باشند؛ هواپیماهای بدون سرنشین (UAV)[1] توانایی شناسایی را بالا برده‌اند؛ ماهواره‌ها نیز به موقعیت‌یابی دقیق، حملهٔ دقیق، ارتباطات و انتقال اطلاعات کمک می‌کنند. درعین‌حال عملیات‌های نبرد اطلاعاتی هم به بخش مهمی از مهارت نظامیان در عصر اطلاعات تبدیل شده‌اند.[۲]

اگرچه تکنولوژی اطلاعات تأثیر مهمی بر عملیات‌های نظامی داشته است، توانایی‌ها و چالش‌های امنیتی به‌واسطهٔ عصر اطلاعات که حوزه‌ای فراتر از میدان جنگ را شامل می‌شود نیز بیشتر شده‌اند؛ برای مثال، رشد بسیار زیاد اقتصاد اینترنتی، بعد تازه‌ای به تجارت بخشیده است؛ بااین‌حال صنایع وابسته به اینترنت نیز با آسیب‌پذیری‌های زیادی روبه‌رو هستند. اقتصاد اینترنت، امنیت اطلاعاتی و وابستگی ساختاری را به‌همراه دارد. حفاظت از اجزای اصلی

---

۱. این متن اقتباسی است از:

Goldman, Emily O., "Security in the Information Technology Age", **Contemporary Security Policy**, Vol. 24, No. 1, April 2003, pp. 1-12.

۲. درخصوص تأثیر عملیات‌های نبرد اطلاعاتی مباحث مختلفی وجود دارد. عملیات نبردهای متحد در سال ۱۹۹۹ برای مجبور ساختن نیروهای صرب به خروج از کوزوو ازسوی برخی متخصصان نظامی به‌عنوان نخستین نبرد اطلاعاتی مورد تحسین قرار گرفت. ایالات متحده برای پشتیبانی از بمباران صربستان، تیمی از جنگجویان اطلاعاتی را با هدف حمله الکترونیکی به شبکه‌های مهم و سیستم‌های کنترل و فرماندهی ایجاد کرد. بررسی‌های صورت‌گرفته پس از نبرد نشان می‌دهد که تلاش‌های نبرد اطلاعاتی به‌طور ناکارآمد مورد استفاده قرار گرفته‌اند.

زیرساخت‌های اطلاعاتی دولتی و خصوصی بدون قاعده‌مند ساختن صنعت ارتباطات و همکاری میان بخش‌های دولتی و خصوصی به‌آسانی امکان‌پذیر نیست.[1]

کنترل و استفاده از اطلاعات و دانش، موتور فعالیت و پیشرفت بشری است. اشخاص، سازمان‌ها و کشورها تعامل بیشتری در فضای اطلاعاتی خواهند داشت؛ درنتیجه رهبران سیاسی، نظامی و اقتصادی تحت فشار بیشتری برای مدیریت، جلوگیری و کاهش سطح مخاطرات ناشی از تکنولوژی اطلاعات قرار خواهند گرفت. تهدیدات پیش روی فضای اطلاعاتی در طیفی از تهدیدات نظام‌مند و پایا تا تهدیدات پراکنده، تصادفی و غیربدخواهانه قرار دارند. تأثیرات کامل انقلاب تکنولوژی اطلاعات بر ثبات جهانی و امنیت ملی هنوز شناخته نشده، ولی آشکار است که عصر اطلاعات تهدیدات، آسیب‌پذیری‌ها و جنگ‌ها را تغییر داده است. این تغییرات نیازمند اقدامات امنیتی جدیدی است. در مواجهه با این چالش‌ها نیز تشکیلات امنیتی ملی به تفکری تازه نیاز دارند. این نوشته از دیدگاه‌های مختلف بررسی می‌کند که چگونه یکی از مهم‌ترین تغییرات اجتماعی در تاریخ (انقلاب تکنولوژی اطلاعات) بر امنیت تأثیر گذارده است. پیشرفت‌های صورت‌گرفته در تکنولوژی‌های اطلاعات کامپیوتری و ارتباطات با نوآوری‌های مدیریتی و ابتکارات در عملکردها و ساختارهای سازمانی همراه بوده است. این تغییرات نیروهایی را به‌وجود آورده‌اند که بسیاری از مفروضات مفهومی و اخلاقی نخبگان امنیت ملی در نیم قرن گذشته را به چالش می‌کشند. انقلاب اطلاعاتی، آسیب‌پذیری را بازتعریف کرده است؛ زیرا هم‌اکنون پیشرفته‌ترین جوامع به‌دلیل وابستگی بسیار به اطلاعات دارای بیشترین آسیب‌پذیری در مقابل حملات هستند. انقلاب اطلاعاتی با پخش و

---

۱. گریگوری رتری در «جنگ استراتژیک در فضای اطلاعاتی» عنوان می‌دارد که فشارها برای کاهش هزینه‌ها به سیستم‌هایی تبدیل شده‌اند که تنها نیازهای عملیاتی عادی را برآورده ساخته، احتیاجات کافی را مورد توجه قرار نمی‌دهند. خرابی تأسیسات سوئیچینگ وریزون در منهتن در زمان حمله به مرکز تجارت جهانی، اختلالات گسترده تلفنی در این منطقه را به همراه داشت؛ برخی اشتباهات برای ماه‌ها ادامه پیدا کرد. در همان زمان انحصار طولانی مدت شرکت AT&T دولت را مجبور نمود تا با اپراتورهای چندگانه در توسعهٔ اقدامات امنیتی همکاری کند.

توزیع قدرت در میان بازیگران دولتی ضعیف‌تر و بازیگران غیردولتی، دوباره به تعریف اینکه چه کسی توانایی تهدید را دارد، پرداخته و درعین‌حال انتظارات راجع‌به درگیری میان جوامع دموکراتیک را نیز تغییر داده است. تجربیات اخیر هم نشان می‌دهد که رأی‌دهندگان نسبت به هرچیزی جز کشتار گسترده بی‌تفاوت هستند.

۲. مدیریت درگیری‌ها در عصر اطلاعات

بازدارندگی، پارادایم استراتژیک در عصر هسته‌ای بود و در مدیریت درگیری‌ها میان دو ابرقدرت ثابت کرد که کاملاً موفق است. دراین‌خصوص ابرقدرت‌ها با یکدیگر جنگ نکرده، بلکه از آن اجتناب ورزیدند. هم‌اکنون نبرد اطلاعاتی[1] دو مشکل مهم را در چارچوب بازدارندگی ایجاد کرده است: سنجش‌پذیری و تناسب. پارادایم بازدارندگی جنگ سرد بر اصل تلافی متقابل تأکید داشت. براین‌اساس خسارات متحمل‌شده در تلافی طرف مقابل به‌اندازهٔ خسارات وارده در حمله به آن است؛ ولی زمانی‌که حمله‌ای، ویرانی ساختمان‌ها یا کشتار مردم را در پی نداشته باشد و صرفاً اطلاعات را نابود سازد، چه می‌توان گفت؟ پاسخ مناسب چه خواهد بود؟ ممکن است ساختار اطلاعاتی دشمن آنچنان برای امنیتش مهم نباشد که هدف مناسبی برای تلافی باشد. پس آیا دراین‌صورت باید در پاسخ، به نابودی فیزیکی دارایی‌های ملی دشمن تهدید نمود؟ آیا حمله به ارتباطات اجتماعی را باید اقدامی در چارچوب جنگ متعارف دانست؟

مدل تلافی متقابل با مشکل تناسب نیز روبه‌روست. ممکن است حملات از سوی یک دولت نبوده، بلکه تروریست‌ها، جنایتکاران یا هکرها دست به این حملات زده باشند (کسانی‌که هویت خود را پنهان کرده، هیچ دارایی برای تلافی برضد آن ندارند). اگرچه ممکن است دولت‌ها به‌واسطهٔ آسیب‌پذیری در نبرد اطلاعاتی از این نوع جنگ بازداشته شوند، بازیگر

1. Information War (IW)

غیردولتی را نمی‌توان با تهدید تلافی از این کار بازداشت. از لحاظ نظری، بازیگران می‌توانند خود را از طرف «بازدارندگی» به طرف «غیربازدارندگی» به‌عنوان بخش جدایی‌ناپذیری از نبرد اطلاعاتی منتقل کنند؛ برای مثال، شرکتی که درگیر جاسوسی صنعتی است می‌تواند به‌جای استفاده از منابع شرکت با یک هکر قرارداد ببندد. دولت‌ها نیز ممکن است برای پنهان ساختن حملات استراتژیک خود به هکرها روی آورند. درعین‌حال حتی می‌توانند وارد «ائتلاف‌های مستحکم» با سازمان‌های غیردولتی (NGOs)، اشخاص ماهر، شرکت‌های چندملیتی (MNCs) و حتی باندهای تبهکاری شوند تا بر یک حمله تأثیرگذار باشند.[1] همان‌طورکه ریچارد هرکنت[2] عنوان می‌دارد، کاهش احتمال یافتن عاملان یک حمله بدان معناست که نمی‌توان صرفاً بر بازدارندگی تأکید داشت، بلکه باید استراتژی‌هایی را توسعه داد که بتوان در این محیط بر مشکلات فائق آمد. حال اگر شرایط مدل سنتی بازدارندگی با محیط نبرد اطلاعاتی همخوانی ندارد، چه نوع مفاهیم استراتژیک را باید جایگزین آن ساخت؟ هرکنت و دیگران برخی از جایگزین‌ها را بیان می‌دارند.

اگرچه بازدارندگی به‌عنوان استراتژی مدیریت درگیری‌ها و جلوگیری از وقوع جنگ مدنظر است، بحران مدیریت ـ که طی جنگ سرد بسیار مورد توجه بود ـ نیز به همان اندازه اهمیت دارد. بحران مدیریت بر جلوگیری از افزایش مناقشات که می‌تواند سرآغازی برای جنگی مهم باشد، تمرکز دارد. چند کارکرد مهم جلوگیری از مناقشات در تکنولوژی اطلاعات عبارتند از: افزایش شفافیت و اعتمادسازی در رژیم‌های کنترل تسلیحات و عملیات‌های برقراری صلح؛ آشکار کردن تجهیزات نظامی و اشاعه اطلاعات برای کاهش حملات غافلگیرکننده استراتژیک؛ ردیابی فعالیت‌های تروریستی و جنایات سازمان‌یافته با ایجاد پایگاه‌های اطلاعاتی جهانی؛ و اشاعهٔ اطلاعات برای مقابله با تحرکات ملی‌گرایانه افراطی که در پی ایجاد درگیری‌های قومی

1. Alvin and Heidi Toffler, “Foreword: The New Intangibles”,In John Arquilla and David Ronfeldt, eds., **Athena’s Camp: Preparing for Conflict in the Information Age**, Santa Monica, CA: RAND, 1997, p. xix.
2. Richard Harknett

و نسل‌کشی هستند.[1]

دامون کلتا[2] تردید دارد که افزایش توانایی‌ها برای جمع‌آوری، تحلیل و توزیع اطلاعات مشکل مدیریت بحران را تسهیل خواهد کرد. منطق شایع آن است که مدیریت بحران شکلی کوچک‌تر از درگیری نظامی است که تأکید دارد همان دستاوردهای ناشی از تکنولوژی‌های انقلابی در میدان نبرد در زمان بحران‌ها نیز قابل حصول هستند. به‌هرحال مدیریت بحران اغلب در مقایسه با جنگ‌ها شرایط خاص خود را دارد. جنگ‌ها برای حذف رقابت صورت می‌گیرند، درحالی‌که مدیران بحران در پی ایجاد همکاری و اجتناب از جنگ هستند. کلتا دراین‌زمینه بیشتر به مهارت دیپلماتیک اعتقاد دارد تا به تکنولوژی.

۳. سازمان‌دهی و هدایت جنگ در عصر اطلاعات

جنگ در عصر اطلاعات نه‌تنها به‌واسطهٔ تکنولوژی، بلکه با مفاهیم و سازمان‌هایی که برای به‌کارگیری این تکنولوژی ایجاد شده‌اند، شکل خواهد گرفت[3] و آینده و چالش آن تا حد زیادی به توسعهٔ مفاهیم و سازمان‌های مورد نیاز برای به‌کارگیری کارآمد تکنولوژی یا حصول به خود تکنولوژی بستگی دارد. در اینجا بررسی دو نکته مهم است: یکی اینکه، ارتش‌ها درحال‌حاضر برای جنگ چگونه سازمان‌دهی می‌شوند و بر چه مفاهیمی تأکید دارند؟ آنها برای جنگ در عصر اطلاعات چگونه باید سازمان‌دهی شوند؟ دوم اینکه، آیا شاهد افول جنگ‌های ویرانگر و افزایش جنگ‌های مختل‌کننده هستیم؟ آیا ارتش‌ها ازکارافتاده‌اند یا اینکه مدل کلاوسویتزی از جنگ‌های ویرانگر همچنان قدرتمند است؟

مدل کلاوسویتزی عصر صنعتی از جنگ ویرانگر، در عصر اطلاعات، توسط مدلی از جنگ

---

1. Joseph S. Nye, Jr. and William A. Owens, "America's Information Edge", **Foreign Affairs**, Vol. 75, No. 2, March-Apr. 1996, pp.20-36.
2. Damon Coletta
3. See Emily O. Goldman and Leslie C. Eliason, **Diffusion of Military Technology and Ideas**, Stanford, CA: Stanford University Press, 2003.

تکمیل خواهد شد که بر اختلال و فلج غیرمرگبار تأکید دارد. تکنولوژی اطلاعاتی را می‌توان به شیوه‌ای ویرانگر همچون در عملیات‌های نظامی برای بهبود کارایی حملات انفجاری نظیر آنچه در عراق شاهد بودیم، به‌کار برد. درعین‌حال می‌توان از آن به شیوه‌ای غیرمرگبار نیز استفاده کرد؛ همچون جایگزینی آن برای حملات انفجاری ازطریق حملات اطلاعاتی که می‌تواند ارتباطات را مختل سازد. از لحاظ نظری، جنگ فلج‌کننده با هدف تضعیف سیستم جنگی دشمن ازطریق شکست جزئی یا کامل کارکرد آن و بدون تخریب صورت می‌گیرد. اگرچه تکنولوژی اطلاعاتی نشان‌دهندهٔ چشم‌انداز آتی از پارادایمی تازه از جنگ است، کریس دمچاک[1] عنوان می‌دارد که تحولات مهمی در ایالات متحده این توسعه را به تأخیر انداخته، یا مانع آن می‌شوند. ارتش این کشور از تکنولوژی اطلاعاتی برای افزایش مرگبار بودن تسلیحات خود استفاده می‌کند و احتمالاً دیگران نیز همین رویه را دنبال خواهند کرد. تحلیل وی سؤالاتی را درمورد ظهور پارادایم‌های تازه‌ای از جنگ مطرح می‌سازد؛ برای اینکه پارادایمی تازه ظهور پیدا کند، چه شرایطی باید وجود داشته باشد؟ زمانی‌که دو پارادایم رقیب در کنار یکدیگر وجود دارند، برای جامعه‌ای که خواهان اتخاذ چارچوب سازمانی جدید و انقلابی کردن شیوهٔ عملیاتی خود است، تنها برتری تکنیکی کافی نیست. چه زمانی گروه‌های سازمانی به لزوم تغییر پارادایم پی می‌برند؟ سرانجام، در زمانی‌که پارادایم‌های قدیم و جدید در کنار یکدیگر وجود دارند، چه الگوهای جنگی را می‌توان انتظار داشت؟

مت بیشاپ[2] و امیلی گلدمن چگونگی همگرایی نبرد اطلاعاتی به‌خصوص حملات اطلاعاتی برضد اهداف فیزیکی و اطلاعاتی را با نبردهای نظامی مورد بررسی قرار داده‌اند. آنها سؤال می‌کنند که آیا منطق استراتژیک جنگ تغییر کرده است یا صرفاً ابزارهای انجام آن؟ و سپس عنوان می‌دارند که علی‌رغم تغییرات چشم‌گیر در تکنولوژی، منطق جنگ همچنان مثل گذشته است (هماهنگی و تسلسل حملات برای دستیابی به اهداف اطلاعاتی به‌عنوان بخشی از

1. Chris Demchak
2. Matt Bishop

نبردی وسیع‌تر و رسیدن به اهداف سیاسی، مادی و سمبلیک). اکثر عملیات‌های نظامی را می‌توان «تسلسلی»[1] یا «انباشتی»[2] دانست. جنگ‌های سنتی (همانند: جنگ‌های اول و دوم جهانی) جنگ‌های تسلسلی بودند. آنها به لحاظ منطقی به درگیری‌هایی مرتبط می‌شدند که به حصول هدفی مشخص و خطی (غلبه بر یک سرزمین نظیر: جبهه غربی در جنگ جهانی اول یا ایجاد پایگاه‌های نظامی) ختم می‌شده است. طی جنگ سرد، بسیاری از درگیری‌های کوچک به‌واسطهٔ استراتژی‌های انباشتی صورت می‌گرفتند. در این زمان کنترل بر سرزمین اهمیت اندکی داشت. در مقابل، تأثیرات انباشتی برخی متغیرها (وارد ساختن تلفات، ره‌گیری تدارکات و ...) مشخص‌کنندهٔ جنگ بود. نبرد اطلاعاتی برای هر دو نوع استراتژی مذکور مناسب است. حملات اطلاعاتی برضد اهداف نظامی را می‌توان نخستین گام در یک استراتژی تسلسلی دانست که برای تسهیل حملات فیزیکی بعدی طراحی شده است. همین‌طور حملات اطلاعاتی علیه اهداف اجتماعی را می‌توان در استراتژی انباشتی به‌کار برد تا ارادهٔ مردم کشور دشمن تضعیف گردد.

ادغام حملات اطلاعاتی در نبردهای نظامی سنتی ممکن است منطق پایان‌دهنده جنگ را به‌دنبال داشته باشد؛ اما این شیوهٔ حمله چالش‌های تازه‌ای را پیش روی متفکران استراتژیک قرار می‌دهد. اگر درگیری، بیشتر مختل‌کننده باشد تا ویرانگر، آنگاه در کجا صلح پایان یافته و جنگ آغاز می‌شود؟ چه نوع فعالیت الکترونیکی به جنگ منجر خواهد شد؟ در حوزهٔ اطلاعاتی، مهارت‌هایی که توانایی ایجاد امکانات دفاعی را موجب می‌شوند (برای مثال، کدگذاری و رمز واژه‌ها) می‌توانند درعین‌حال برای شنود، آلوده کردن یا اختلال جریانات اطلاعات نیز مورد استفاده قرار گیرند. با توجه به توان تکنولوژیکی برای نفوذ، انگیزه زیادی برای ایجاد اختلالات در جهت «آماده کردن میدان نبرد» قبل از آغاز خصومت‌های متعارف یا بحران‌ها وجود دارد تا سیستم جنگی دشمن از کار بیفتد. نرم‌افزارهای رایانه‌ای که رایانه‌ها را

---

1. Sequential 2. Cumulative

مختل می‌کنند، به‌عنوان اقدامی خطرناک یا اقدامی جنگی به حساب نمی‌آیند؛ ولی باید گفت که ایجاد اختلال می‌تواند به اندازهٔ ویرانگری، تهدید امنیتی بزرگی محسوب شود. آیندهٔ تکنولوژیکی نبرد اطلاعاتی، مرزهای جنگ و صلح را از بین برده، اصول سنتی تهاجم و دفاع را به چالش می‌کشد. در نبرد اطلاعاتی، میدان نبرد کجاست؟ کدام عملیات‌ها اقدامات دفاعی مشروع و کدامیک تهاجمی هستند؟

سرانجام، جنگ در عصر اطلاعات مباحثی در مورد هموار شدن راهبردی جنگ توسط تکنولوژی اطلاعاتی و تبدیل اشخاص به بازیگرانی مرگبار (همچون دولت‌ها) را موجب شده است. به‌عقیده هرکنت، افرادی اندک می‌توانند جهنمی بزرگ را ایجاد کنند. بیشاپ و گلدمن این نکته را رد نمی‌کنند؛ ولی تأکید دارند که تنها دولت‌ها و گروه‌های مورد حمایت آنها قادر به انجام حملات بزرگی خواهند بود و بنابراین از مزیت قابل توجهی نسبت به اشخاص و گروه‌های کوچک برخوردار هستند.

۴. حاکمیت در عصر اطلاعات

اگر استراتژی به رابطهٔ ابزار و امکانات برای رسیدن به اهداف مربوط می‌شود، باید بازتابی از ارادهٔ مردم باشد. حمایت مردمی در کانون چگونگی سازمان‌دهی دموکراسی برای امنیت ملی، نحوه تصمیم‌گیری رهبران منتخب برای وارد شدن به جنگ و چگونگی هدایت آن قرار دارد. یکی از تأثیرات مهم انقلاب اطلاعاتی را می‌توان توانایی جنگیدن با تلفات و خسارات کمتر از گذشته دانست. بااین‌وجود توانایی‌های نبرد اطلاعاتی ارتش‌های دموکراتیک، مسئولیت‌پذیری و حریم خصوصی را مورد مصالحه قرار می‌دهد که این موارد از سوی میراسلاو نینسیک[1] و پت مورگان[2] مورد بررسی قرار گرفته است.

نینسیک سه دلیل محدودکنندهٔ دموکراتیک از سوی نبرد اطلاعاتی را به‌صورت زیر بیان

1. Miroslav Nincic 2. Pat Morgan

می‌دارد: نبرد اطلاعاتی با ازبین بردن مرزهای جنگ و صلح، جلوگیری از وقوع جنگ از سوی مردم و نمایندگانشان را مشکل‌تر می‌سازد. نبرد اطلاعاتی با تحریف اطلاعات در جهت سردرگم‌کردن دشمن، ممکن است برعکس سبب فریب مردم شود که همین امر کنترل مردم را که قلب حاکمیت دموکراتیک هستند تحلیل می‌برد. در نهایت، نبرد اطلاعاتی به دولت اجازه می‌دهد تا در زندگی خصوصی شهروندانش بیش‌ازحد مداخله کند. مورگان با تمرکز بر این نکته عنوان می‌دارد که تنشی منطقی میان حریم خصوصی و امنیت وجود دارد. امنیت دسترسی به اطلاعات مربوط به جنایتکاران و تهدیدات خارجی را الزامی می‌سازد. حریم خصوصی به‌معنای عدم دسترسی و نفوذ به زندگی شهروندان عادی است. توسعه جمع‌آوری اطلاعات، پردازش و انتقال آن، تهدید حریم خصوصی را در کنار تهدیدات فریب و کنترل افزایش داده است. وی به‌ویژه از این مسئله نگران است که توانایی‌های نفوذ با هدف امنیت ملی در برابر سیستم‌های اطلاعاتی و ارتباطاتی خارجی، در کنار افزایش نظارت‌ها به دلایل امنیت داخلی یا دیگر دلایل، احتمال سوءاستفاده را ازسوی ناظران امنیتی که تحت نظارت مردمی نیستند افزایش دهد.

تهدید حریم خصوصی به دو دلیل، دیگر به سادگی از کنترل‌های دولتی محسوب نمی‌شود: اول اینکه، انقلاب ارتباطاتی مشکل امنیت داخلی را جهانی ساخته است. سوءاستفاده از تکنولوژی جدید به هرکس اجازه می‌دهد حریم خصوصی دیگران را نقض کرده، به‌آسانی از موانع و مقررات داخلی فرار کند. دوم اینکه، گسترش توانایی‌های نفوذ به زندگی خصوصی دیگران نظارت کنترل‌نشده را چند برابر می‌سازد. از لحاظ داخلی، انباشت اطلاعات شخصی حساس در دست بخش‌های دولتی و خصوصی همچنان ادامه دارد و اقدامات و شیوه‌های گوناگون برای جلوگیری از دسترسی و سوءاستفاده از آن ناکافی و مشکل است.

پیوستگی امنیت و حریم خصوصی یکی از مهم‌ترین مسائلی است که رهبران سیاسی باید به آن توجه داشته باشند. پیش‌ازاین بیست شهر ایالات متحده مصوباتی را به تصویب رسانده‌اند که قانون وطن‌پرستی این کشور را تهدیدی برای حقوق مدنی اعلام کرده، در برخی

موارد از کارکنان دولتی خواسته‌اند که با مأموران فدرال همکاری نکنند.[1] اگر کشف و اقدام پیشگیرانه زیربنای دفاع در مقابل نبرد اطلاعاتی و نیز دیگر حملات باشد، آنگاه جامعه چگونه باید نگرانی‌های خود را برای حریم خصوصی و امنیت تعدیل نماید؟ در جوامع دموکراتیک این پاسخ‌ها به برداشت‌های عمومی از تهدیدات پیش روی امنیت و حریم خصوصی مربوط می‌شود. اگرچه نگرانی مردم درخصوص چگونگی نقض هنجارهای دموکراتیک به‌واسطهٔ نبرد اطلاعاتی رو به افزایش است، اینکه جنگ‌های مختل‌کننده جایگزین جنگ‌های ویرانگر می‌شوند، کسب حمایت مردمی را از چنین عملیات‌هایی آسان‌تر می‌سازد. جنگ «دقیق» می‌تواند شمشیری دو لبه باشد: مردم انتظار تلفات و خسارات کمتر و دقت بیشتر در کشف، بازدارندگی و پاسخ به حملات را دارند؛ ولی این امر ممکن است به‌معنای نقض هنجارهای دموکراتیک حریم خصوصی و مسئولیت‌پذیری باشد.

---

1. **"Tow More Cities May Join Patriot Act Revolt",** <http://abcnews.og.com/sections/us/Daily News/usapatriot_oakland021217.html>.

فصل دوم
مبانی نبرد اطلاعات

- نظریه‌های نبرد اطلاعات
- مفهوم‌شناسی اطلاعات
- مفهوم‌شناسی نبرد
- نبرد و ارتباط آن با آنچه می‌دانیم یا اعتقاد داریم
- کارکردهای نبرد اطلاعات
- ویژگی‌های نبرد اطلاعات استراتژیک
- منابع در نبرد اطلاعاتی

۱. نظریه‌های نبرد اطلاعات

جان ارکیلا[1] و دانلد رانلفت[2] ـ که از نخستین و زبده‌ترین نظریه‌پردازان نبرد اطلاعاتی هستند ـ مقالات ارزشمندی را تهیه کرده‌اند که بخش عمده آنها مربوط به مفاهیم دو قلوی «جنگ اینترنتی» و «جنگ شبکه‌ای» است. به گفته این نویسندگان، منظور از جنگ سیبرنتیک یا اینترنتی، سیطره غنی‌شده اطلاعاتی از جنگ نظامی آینده است که در آن، تلاش و مبارزه برای برتری اطلاعاتی، اهمیت حیاتی پیدا می‌کند. جنگ شبکه‌ای ـ که تأثیرگذارترین نوع جنگ آینده است ـ به مناقشاتی میان اجتماعی از مفاهیم و پیام‌های ملی اطلاق می‌گردد. در میان نظریه‌پردازان و صاحب‌نظران، این دو تن به‌دلیل مقایسه‌ای که میان نبرد اطلاعاتی و سیطره‌های «گردن‌زنی» و معمول میان قبایل مغول در قرن سیزدهم میلادی انجام داده‌اند، از دیگران شناخته‌شده‌تر هستند. آنها از سرعت برتر و خطوط ارتباطی به‌عنوان ابزار کنترل دشمنی استفاده کردند که از لحاظ تعداد آرا، برتر و در منطقه وسیعی پراکنده بودند. از لحاظ آرمانی، جنگ سیبرنتیک به شبکه‌ای از جنگجویان اطلاعاتی غیرمتمرکز امکان می‌دهد که ازطریق هدف‌گیری مستقیم مرکز عصبی اطلاعات دشمن و اقدام به نوعی حمله برق‌آسای دوران فراصنعتی، به پیروزی قطعی و بدون خونریزی دست یابند. ازهمین‌لحاظ جنگ شبکه‌ای نیز ممکن است با فراهم ساختن امکان موضع‌گیری بازدارنده‌تر و اعمال کنترل بر مفاهیم و ادراکات دشمن، از به‌راه افتادن جنگ‌های واقعی (یا جنگ‌های سیبرنتیک)

---

1. John Arquilla

2. David Ronfeldt

جلوگیری به‌عمل آورد.

گروه دیگری از نظریه‌پردازان (جورج استاین[1]، ریچارد زافرانسکی[2] و اون جانسون[3]) معتقدند که بزرگ‌ترین پتانسیل نبرد اطلاعاتی عبارت است از: قلمرو تازه‌ای از جنگ که در آن اطلاعات (یا دانش) به‌خودی‌خود هم مرکز ثقل و هم اسلحه اصلی است. اگر از بعد منطقی به آن بنگریم باید گفت که این نوع جنگ آینده‌گرایانه در محیط تغییرشکل‌یافته عصر اطلاعات و به کمک جنگ‌افزارهایی انجام می‌پذیرد که می‌دانیم اکنون اغلب از رده خارج شده‌اند. این امر، نه میدان جنگ دیجیتالی و نه نوع سوزن‌دوزی‌شده‌ای از اطلاعات و تکنولوژی بر روی سیستم‌های موجود، بلکه موضوعی انقلابی و کاملاً متفاوت است.[4]

در توضیح دیدگاه‌های برخی از این نظریه‌پردازان باید گفت که طبق نظریه انقلابی نبرد اطلاعاتی ممکن است نقش استراتژیک برای آن، یعنی چیزی ورای برنامه کاربردی جنگ فرماندهی و کنترل به‌عنوان مضاعف‌کننده نیرو، شبیه به نقش قدرت هوایی استراتژیک در جنگ‌های اطلاعاتی متصور گردد. تکنولوژی‌های درحال ظهور اطلاع‌رسانی به ما امکان می‌دهند تا ازطریق انجام تبلیغات مستمر با فکر و اندیشه دشمن به نبرد پرداخته، واقعیت را به دنیایی تخیلی که ازطریق شبکه‌های اطلاع‌رسانی متعدد به آنها خدمت ارائه می‌گردد، بدل نماییم. بنابراین همانند مفهوم جنگ شبکه‌ای، نبرد اطلاعاتی نیز نوع پیشرفته‌تری از تبلیغات و عملیات روان‌شناختی است که در آن از تکنولوژی برتر استفاده می‌شود. این تبلیغات و عملیات، توده‌ها یا برخی مخاطبان خاص را هدف قرار می‌دهند.

درواقع به منظور کنترل دشمن ازطریق برتری و استیلای اطلاعات استراتژیک، برای دست‌کاری در اطلاعات آن تا با منافع ما متناسب شود، و شرطی نمودن دانش و شناخت آن از موقعیت تا در بهترین وضعیت بدون اطلاع و آگاهی آن انجام گیرد، از تکنولوژی پیشرفته

---

1. George Stein
2. Richard Szafranski
3. Owen E. Jenson
4. Richard Szafranski, "A Theory of Information Warfare: Preparing for 2020", **Airpower Journal,** Vol. 9, No. 1, Spring 1995, PP. 58-59, 62.

اطلاع‌رسانی استفاده می‌شود.[1]

مارتین لیبیکی، از اندیشمندان بارز موضوع نبرد اطلاعاتی ـ که بیش از همه در راستای پر کردن شکاف بین نظریه و عمل تلاش کرده ـ به‌تازگی اظهار داشته است که اطلاعات ممکن است سرانجام به عامل اصلی بازدارنده جنگ تبدیل شود و علت این امر شفافیت جهانی است که به کمک آن پدید می‌آید. شبکه‌ای از ماهواره‌ها و رادارهای زمین‌پایه، هواپایه و دریاپایه دور کره زمین را احاطه کرده و تمام نقاط جهان و فعالیت‌های آن زیر ذره‌بین قرار خواهد گرفت. یک زیرساخت اطلاعاتی جهانی کاربران این اطلاعات را به‌هم مرتبط خواهد ساخت و نوعی آگاهی عمومی از اقدام امنیت نظامی و امثال آن را موجب خواهد شد. تحت چنین شرایطی، هرگونه جابجایی و تحرک مرزی یا سازمان‌دهی و بسیج ناگهانی نیرو در معرض دید قرار داشته، در اسرع وقت، ازطریق تهدید متجاوز بالقوه، با آن مقابله خواهد شد. درصورت اصرار و پافشاری متجاوز، جامعه بین‌المللی تنها کاری که خواهد کرد این است که شریان‌های حیاتی متجاوز را که اقدام جنگی، اقتصاد و زیرساخت‌های ملی آن به آنها وابسته است، قطع کند و درواقع بدون آنکه حتی یک گلوله شلیک شود، او را به زانو در آورد.[2]

بسیاری از این نویسندگان به‌صورت ذهنی راه‌های تازه اندیشیدن درباره جنگ و جنگیدن در عصری از تحول و دگرگونی را مورد بررسی قرار می‌دهند. برای جلوگیری از مقاومت در برابر نوگرایی و تحول همواره به کمک اندیشه‌ها و چشم‌اندازهای نوین نیاز است. مفروضات بسیاری از این نظریه‌پردازان تا حد زیادی به نوآوری‌های تکنولوژیکی عصر حاضر بستگی دارد. حتی با تأکید بر اینکه هدف واقعی نبرد اطلاعاتی، فکر انسان است، چیزی که یادآور خرد و حکمت کهن «سان تزو» است، باید گفت تصوری که آنان ایجاد می‌کنند، بدون به‌کار بردن عنوان کاملی از تکنولوژی‌های نوین و درحال ظهور در دنیای کاملاً به‌هم پیوندخورده

1. Martin Libicki, "The Emerging Primacy of Information", **Orbis**, Vol. 40, No. 2, Spring 1996, pp. 261-276.
2. Andrew Krepinevich, "Cavalry to Computer: the Pattern of Military Revolutions", **The National Merest**, No. 37, Fal 1994, pp.30-42.

عصر اطلاعات، غیرممکن می‌نماید. در مورد توان نبرد با دشمن یا بازداشتن آن از هرگونه اقدامی در فضای سیبرنتیک و با استفاده از ابزارهای اینترنتی پیش‌بینی می‌شود که دشمن نیز به اندازه خود ما، به تکنولوژی‌های اطلاع‌رسانی متکی است. تهدید به قطع ارتباطات دشمن مؤثر واقع نخواهد شد، مگرآنکه وی برای بقای خود به‌کلی به آن وابستگی داشته باشد و ما نیز به‌نوبه‌خود توان قطع کردن آنها را داشته باشیم. تبلیغات تلویزیونی علیه دشمنی که دارای تلویزیون ماهواره‌ای یا ارتباط اینترنتی نباشد چه فایده‌ای دارد؟ در سال ۱۹۹۷ نیمی از مردم جهان حتی یک‌بار هم از تلفن استفاده نکرده بودند. به‌همین‌ترتیب دست زدن به عملیات روان‌شناختی، صرف‌نظر از اینکه از چه تکنولوژی‌های پیشرفته و فراگیری استفاده شده باشد، درباره حکومت‌های خودکامه‌ای که درحال‌حاضر نمایانگر بسیاری از چشمگیرترین تهدیدهای امنیتی هستند، به‌هیچ‌وجه تأثیرگذار نخواهد بود. درواقع جالب است که چنین استراتژی‌ای ممکن است برای نظریه‌پرداز آمریکایی جاذبه داشته باشد؛ زیرا این جامعه بسیار دموکراتیک، اشباع از رسانه و ازلحاظ فناوری پیشرفته است که بیشترین آسیب‌پذیری را در برابر چنین حمله‌ای دارد.[۱]

برخی از متفکران و اندیشمندان نبرد اطلاعاتی کوشیده‌اند تا با گفتن اینکه «لازم نیست برده‌وار دنباله‌روی موج فناوری باشیم» خویشتن را از اتهامات جزم‌گرایی تکنولوژیکی محفوظ نگاه دارند. آنان معتقدند که به‌جای این پیروی برده‌وار، باید افکار خویش را به‌کار اندازیم تا ببینیم از این تکنولوژی می‌خواهیم چه کار برای ما انجام دهد و سپس تکنولوژی متناسب با نیاز خود را به‌وجود آوریم. این امر این واقعیت را که توسعه تکنولوژی، همانند تنظیم استراتژی و تاکتیک‌ها، فرایندی تکاملی است، نادیده می‌انگارد. تکنولوژی‌های نوین پدید می‌آیند که مورد استفاده قرار گیرند یا ضعف‌های تکنولوژی‌های موجود را جبران نمایند. ارائه

---

1. **Steven Metz and James Kievit, Strategy and the Revolution in Military Affairs: From Theory to Policy**, Carlisle Barracks, Pa : Strategic Studies Institute, U.S. Army War College, 1995.

نظریه نبرد اطلاعاتی به‌طور مجرد خطر سقوط به ورطه نوعی اشتباهات را دربردارد.[1]

یک انقلاب نشئت‌گرفته از تکنولوژی در امور نظامی بار دیگر فکر و ذهن متفکران و اندیشمندان نظامی پیشرو را به خود مشغول داشت: نبرد اطلاعاتی موضوعی است که هسته مرکزی این تازه‌ترین انقلاب در امور نظامی را تشکیل می‌دهد. باز هم خطری که وجود دارد این است که تکنولوژی، کنترل کامل این انقلاب را به‌دست خواهد گرفت و مفاهیمی پدید خواهد آورد که در تئوری کاربرد مستمر دارد؛ اما در عمل با مشکلات بسیاری مواجه است. اگرچه تمسک به عظمت نوآوری‌های تکنولوژیکی حائز اهمیت بسیار است، خطرها، آسیب‌پذیری‌ها و نیازهای واقعیت امنیتی ملی نیز مطرح می‌گردد و تکنولوژی نیز به‌صورت جایگزینی برای استراتژی درنمی‌آید. انقلاب‌های انجام‌گرفته در امور نظامی پدیده‌های موقت هستند و گاهی در مدت کمتر از یک نسل ازبین می‌روند.

برخی نظریه‌پردازان از زمان پیدایش جنگ پیاده‌نظام تا پدید آمدن جنگ‌افزارهای هسته‌ای تعداد ده انقلاب را در امور نظامی برشمرده‌اند. برخی دیگر، انقلاب‌های انجام‌گرفته در امور نظامی را به دو دسته بزرگ و کوچک تقسیم می‌کنند که دسته اول بیشتر تحت تأثیر تکنولوژی قرار داشته، انعطاف‌پذیرند و دسته دوم، یعنی انقلاب‌های کوچک با نظریات تافلری سازگار بوده، بیشتر بر امواج اقتصادی سوارند.[2]

به مرور زمان، تعداد کثیری از تکنولوژی‌های خاص تأثیر چشمگیری بر رهبری جنگ وارد ساخته‌اند؛ نظیر: باروت، موتورهای درون‌سوز، مکانیسم‌های ته‌پر، بی‌سیم، رادار و نظایر آنها. در زمان ماکیاولی، پیشرفت در بخش توپخانه مشتاقان را برآن داشت تا پیش‌بینی کنند که این ابزار جای سایر جنگ‌افزارها را خواهد گرفت؛ اما تا پانصد سال بعد هم این پیش‌بینی هنوز تحقق نیافته و توپخانه همچنان در حال توسعه است. بنابراین شاید گزاف باشد که انتظار داشته باشیم حتی انقلاب‌های واقعی در امور نظامی و تکنولوژی‌های واقعاً انقلابی جدید به تحولات

---

1 Omer Bartov, **Hitler's Army**, Oxford: Oxford University Press, 1992.

2. Michael Howard, **War in Eurppean History**, Oxford: Oxford University Press, 1976, p. 130.

عمده‌ای در درازمدت منجر گردند (خوراک فکری کسانی که انقلاب در امور نظامی اطلاعات پایه فعلی را تحول بزرگ تاریخی می‌دانند).

انقلاب‌هایی که در گذشته در امور نظامی به‌وقوع پیوسته‌اند، گهگاه امتیازات نظامی کوتاه‌مدت قابل توجهی به‌دست می‌دهند. نمونه‌ای که در قرن حاضر بارها از آن یاد می‌شود، حمله برق‌آسای آلمان در جریان جنگ جهانی دوم است که در آن نیروهای زرهی متحرک، ارتباطات رادیویی و پشتیبانی هوایی تاکتیکی به‌طور چشمگیری در لهستان، کشورهای جنوب اروپا و فرانسه در طول سال‌های ۳۹ ـ ۱۹۴۰ درهم آمیخته شدند. برخی تحلیلگران خاطرنشان ساخته‌اند که انقلاب اطلاعات رخ‌داده در امور نظامی می‌تواند توان انجام حمله برق‌آسا را به نیروهای آمریکایی بدهد. بنابراین یادآوری واقعیت سرنوشت ارتش آلمان در جبهه شرقی بعد از ۱۹۴۱ حائز اهمیت بسیار است. وقتی‌که آلمانی‌ها در عمق خاک شوروی بیشتر پیش رفتند، قطار تدارکاتشان دیگر کفاف نیازهای آنها را نمی‌داد و ارتش درواقع جنبه مدرنیزه خود را ازدست داد. حمله برق‌آسای آنها به‌زودی از هم پاشید و جنگ در شرق به نبردی کند، خشونت‌آمیز و فرسایشی تبدیل شد. این حمله به مهمات و تدارکات بسیار نیاز داشت و برای حفظ ارتباطات، تحرک و توان عملیاتی خود به تجدید تدارکات مستمر وابسته بود. نکته هشدارآمیز دیگر برای شرکت‌کنندگان در نبرد اطلاعاتی آن است که در جنگ آینده، یعنی یک جنگ تخیلی (همانند جنگی که مثلاً در سال ۲۰۲۰ اتفاق بیفتد) با شرکت آمریکا و حریفی هم‌توان، حمله لیزری غافلگیرکننده‌ای مجهز به سیستم GPS شناسایی ماهواره‌ای مستقر در آمریکا انجام، و امکانات ارتباطی و سپس یک بمب الکترومگنتیک هسته‌ای (EMP) در فضا منفجر شود و درنتیجه به زیرساخت اطلاع‌رسانی نظامی پرزرق‌وبرق آمریکا که اکثر سیستم‌های تسلیحاتی جدید این کشور به آن وابسته است، آسیب وارد سازد و بیش از پنجاه درصد آن را در همان شروع جنگ از کار اندازد.

پیش‌بینی‌های مربوط به تأثیر تکنولوژی در اکثر موارد، نادرست است؛ حتی هنگامی‌که

تکنولوژی به‌کار گرفته‌شده نشان می‌دهد کاملاً انقلابی است؛ برای مثال، هواپیما، پیروزی تکنولوژیکی بی‌نظیری که بعد تازه‌ای به فضای جنگ بخشید و برای آن تحولی واقعی در جنگ پدید آورد، در برخی نبردها کارساز نیست.

کلاوزوتیس به کرات یادآور می‌شود که سنجش عوامل انسانی جنگ، فوق‌العاده دشوار است. اگر احتیاج ما اختراع باشد، می‌توان گفت که تاکتیک‌های نامتقارن، استراتژی یا ضدتدبیرهای تکنولوژیکی همواره طرح‌های مبتنی بر تکنولوژی را مختل خواهد ساخت. گمان می‌رفت جنگ‌افزارهای هسته‌ای نیز تسلیحات متعارف را از رده خارج ساخته، جنگ را به‌کلی متحول نمایند. استراتژی «مقابله به‌مثل جمعی» دوره آیزنهاور به‌دلیل استقرار آنها، امکانات متعارف را نادیده گرفت؛ اما دریافت که «اراده» به‌کارگیری جنگ‌افزارهای انهدام جمعی، مؤثر واقع نشد. به‌رغم وجود زرادخانه هسته‌ای مهیب، خطر برخی اقدامات ویرانگرانه و جنگ‌های کثیف کوچک در مناطق پیرامون همچنان ادامه یافت و چریک‌ها نیز اینجا و آنجا سربرآوردند. در کره و بعدها ویتنام خواسته شد به تهدید عمل شود. جنگ‌افزارهای هسته‌ای همچنان بدون استفاده ماندند و در غروب عصر صنعتی، سربازان همچنان با همان ترس و وحشتی مواجه بودند که همتاهایشان در جریان جنگ‌های ناپلئون.

مزایای تکنولوژیکی در جنگ به‌طورکلی بسیار زودگذر بود، علاوه‌برآن هیچ استراتژی یا نظریه (مبتنی‌بر تکنولوژی) جنگ را نمی‌توان برای مدتی طولانی حفظ کرد. جنگ‌افزارهای قدیمی نیز الزاماً از رده خارج نمی‌شوند و ابزارهای جدید فقط به آنها افزوده می‌گردند.

نیروهای مسلح در یک دموکراسی از نظارت یا ملاحظه جهت‌گیری آن، حتی در زمان جنگ مستثنی نیستند. جایی‌که اراده مردم، روحیه و تکنولوژی همگی در سطح بالایی قرار دارند، نیروهای مسلح بسیار سودمند و باارزش خواهند بود. به‌هرحال اگر روحیه از بین برود، تأثیری دومینومانند روی خواهد داد: حمایت مردمی، سطح بالای تکنولوژی و نیروهای مسلح

به‌دنبال هم ازبین خواهند رفت. دراین‌راستا متن حاضر تئوری نبرد اطلاعاتی[1] را در چارچوب گسترده‌تری از جنگ مطرح نموده، شیوه‌هایی را برای نبرد اطلاعاتی در سطوح استراتژیک عملیاتی ارائه می‌دهد. ابزارهای مورد نیاز برای نبرد اطلاعاتی موجود است و ازآنجایی‌که تسلیحات اطلاعاتی بسیار قدرتمند هستند، باید نظامیان و غیرنظامیان را در مقابل آنها مورد محافظت قرار داد. آسیب‌پذیری در برابر نبرد اطلاعاتی، حالتی جهانی دارد. تصمیمات اتخاذشده برای توسعه تسلیحات اطلاعاتی یا استفاده از نبرد اطلاعاتی همگی تصمیماتی دولتی هستند. این تصمیمات باید آگاهانه و با درک کامل از مخاطرات اخلاقی و روحیه‌ای آن اتخاذ گردند. پس از بررسی تمام مخاطرات و تصمیم‌گیری برای ساخت تسلیحات اطلاعاتی یا شروع یک نبرد اطلاعاتی، تصمیم‌گیرندگان باید قبل از شروع جنگ یا استقرار تسلیحات، درک روشنی از این تسلیحات و تئوری استقرار تسلیحاتی داشته باشند.

۲. مفهوم‌شناسی اطلاعات [2]

اطلاعات در اینجا به معنای «محتوا یا معنی یک پیام است».[3] هدف از جنگ‌ها همیشه تأثیرگذاری بر سیستم‌های اطلاعاتی دشمن بوده است. در معنای گسترده‌تر، سیستم‌های اطلاعاتی دربردارنده نوعی وسیله یا شیوه‌ای هستند که بدان طریق بتوان به آگاهی یا اعتقادات خاصی دست پیدا کرد. در معنای محدود آنکه سیستم‌های اطلاعاتی شیوه‌هایی

---

۱. برخی مواقع به‌اشتباه نبرد اطلاعاتی را همان نبرد فرماندهی و کنترل یا C2W می‌پندارند. هدف C2W عبارت است از: بهره‌گیری از حملات فیزیکی و رادیو الکترونیکی برضد سیستم‌های اطلاعاتی دشمن برای جدا کردن نیروهای دشمن از رهبری آن. ازنظر تئوری، نبرد اطلاعاتی مجموعه بسیار بزرگ‌تری از فعالیت‌هاست که ذهن و اراده دشمن را هدف قرار می‌دهد.

۲. این متن اقتباسی است از:

Richard Szafranski (Colonel), USAF, "A Theory of Information Warfare: Preparing for 2020", **Airpower Journal**, 1995

3. Chris Mader, **Information Systems: Technology, Economics, Applications**, Chicago: Science Research Associates, Inc., 1974, p. 3.

هستند که توسط آنها بتوان کنترل خود را بر نیروهای مستقر اعمال کرد. در کل، سیستم‌های اطلاعاتی مجموعه‌ای کامل از دانش، اعتقادات و فرایندهای تصمیم‌گیری دشمن هستند. نتیجه مطلوب نیز آن خواهد بود که دشمن پیام‌هایی را دریافت کند که او را به توقف جنگ متقاعد سازد.

چرا حریف مقابل، جنگ را متوقف خواهد کرد؟ در اینجا شماری از احتمالات وجود دارد: ناتوانی در کنترل نیروها، ازدست دادن روحیه، آگاه شدن از اینکه قدرت نبرد خود را از دست داده است یا آگاهی از اینکه دستاوردهای توقف جنگ بیشتر از تداوم آن خواهد بود. این پیام‌های «متوقف‌کننده جنگ» در محتوا و معنا بسیار متفاوت از یکدیگر هستند؛ نظیر: «دشمن شما را نابود کرده است»، «یا تسلیم شوید یا بمیرید»، «ضدحمله شما با شکست روبه‌رو شده است» یا «مردم کشورتان در جنگی که کودکان کشته می‌شوند از شما حمایت نمی‌کنند». اگرچه شیوه‌های انتقال پیام‌های متوقف‌کننده جنگ طی سال‌ها تغییر کرده است، معنای پیام همچنان ثابت و بدون تغییر مانده است: «جنگ را متوقف کنید».

با تکامل نهادهای اجتماعی از موج اول جوامع کشاورزی به موج دوم کشورهای صنعتی، سیستم‌های اطلاعاتی تکامل یافته، فرایندهای تصمیم‌گیری نیز پیچیده‌تر شدند. سازمان‌های تجاری در داخل و در کنار ساختمان‌های سیاسی مسلط ظهور یافتند و با گسترش حوزه فعالیت‌هایشان، پیچیدگی بیشتری را ایجاد کردند. شبکه‌های کسب اطلاعات کارکنان اطلاعاتی به‌عنوان جدیدترین شکل از ساختار نهادی نیز ظاهر شدند و با پیشرفت ابزارهای تکنولوژی اطلاعاتی، شمار آنها افزایش یافت. با پیشرفت تکنولوژی اطلاعاتی، سیستم‌های اطلاعاتی افزایش کارایی تمام اشکال نهادی دیگر را نیز موجب شدند.[1]

با تکامل نهادهای اجتماعی، شیوه‌های نبرد و جنگ این جوامع نیز تکامل یافت. استفاده از

---

[1]. موج‌های جوامع توسط الوین تافلر در کتاب ذیل توصیف شده‌اند:

Alvin Toffler, **The Third Wave** London: Collins, 1980. See also Alvin and Heidi Toffler, **War and AntiWar: Survival at the Dawn of the 21st Century**, Boston: Little, Brown, 1993.

طبل‌ها، پرچم و سازهای وحشت‌زا در جنگ‌های موردنظر سان تزو که بعدها به‌واسطه تکنولوژی اطلاعاتی پیشرفته شدند، به پیچیده‌ترین عملیات‌های روانی در جنگ‌های مدرن تبدیل گشتند. به گفته جان آرکیلا[1] و دیوید رانفلت[2]، هدف جنگ از نابودی به کنترل تغییر پیدا کرده است.[3] تکنولوژی اطلاعاتی هم‌اکنون به مرحله‌ای از تکامل دست یافته است که می‌تواند با خشونت فیزیکی یا خونریزی اندک، «کنترل» خود را بر دشمن تحمیل نماید. در ظاهر این امر چیز خوبی است، ولی دقیق‌تر که نگاه می‌کنیم به خطرهای آن نیز پی می‌بریم. بررسی دقیق‌تر، جنبه‌های مختلف این امر را نشان خواهد داد.

۳. مفهوم‌شناسی نبرد[4]

نبرد مجموعه‌ای از تمام فعالیت‌های مهلک و غیرمهلک است که برای غلبه بر اراده حریف یا دشمن انجام می‌شود. دراین‌معنا نبرد، مترادف «جنگ»[5و6] و نیازمند اعلام جنگ نیست و درعین‌حال با شرایطی‌که «وضعیت جنگی» نامیده می‌شود، همراه نمی‌گردد. نبرد می‌تواند از سوی گروه‌های دولتی، مورد حمایت دولتی یا غیردولتی یا برضد آنها صورت گیرد. هدف از نبرد لزوماً کشتن دشمنان نیست، بلکه فقط مهم تحت کنترل درآوردن آنان است. در حقیقت، «اوج مهارت» آن است که بتوان بدون کشتن حریف او را تحت کنترل خود درآورد.[7] زمانی‌که

---

1. John Arquilla
2. David Ronfeldt
3. John Arquilla and David Ronfeldt, "Cyberwar is Coming!" **Comparative Strategy,** No. 2, Apr-June 1993, pp.141-165.
4. Warfare
5. War
6. Martin van Creveld, **The Transformation of War,** New York: Free Press, 1991, pp. 196-205.
واژه‌هایی نظیر: جنگ و مبارز جنگی به‌دلیل استفاده نادرست، با واژه جنگجو در یک دموکراسی اشتباه می‌شوند. در ایالات‌متحده «جنگ» توسط کنگره (افرادی که نماینده تمام مردم هستند) اعلام می‌شود. «قدرت‌های جنگی» اجرایی نیز در حقیقت «قدرت‌های نبرد» هستند. به گفته وان کرولد دوران جنگ‌های سه‌گانه عصر کلاوسویتزی به اتمام رسیده، ولی دوران نبرد پایان نیافته است.
7. Sun Tzu, **The Art of War,** trans. Samuel B. Griffith, New York: Oxford University Press, 1971, p. 77.

حریف به شیوه‌ای رفتار می‌کند که ما می‌خواهیم، نشان‌دهنده کنترل بر اوست.[1] برای رسیدن به این هدف باید درک روشنی از رفتارهای غیرخصمانه‌ای که خواهان تحمیل آنها یا رفتارهای خصمانه‌ای که خواهان جلوگیری از آنها هستیم، داشته باشیم.

زمانی‌که نیروهای امنیتی دولتی در نبرد با دشمن وارد می‌شوند، آن دولت رفتارهای غیرخصمانه‌ای را که باید بر دشمن تحمیل شوند مشخص می‌کند. هنگامی که دیگر گروه‌ها (چریک‌ها، باندها، دسته‌ها) درگیر در نبرد می‌شوند، رهبر گروه رفتارهای غیرخصمانه را تعیین می‌کند. در هر دو شکل نبرد دولتی و غیردولتی، تصمیمات اتخاذشده ازسوی رهبران گروه، معرف اهداف، شیوه‌ها و شرایط پس از نبرد هستند. به‌همین‌صورت اظهار اینکه «دولت‌ها» یا «گروه‌ها» به نبرد می‌پردازند، تصور نادرستی است. تصمیم برای ورود به نبرد، ازجمله تصمیم برای پایان آن، ازسوی رهبران در دولت‌ها یا گروه‌ها اتخاذ می‌شود. بااین‌توصیف اراده خصمانه رهبران دشمن است که باید تحت کنترل درآید و همین امر موفقیت نبرد را نشان می‌دهد.[2] اعضای گروه یا شهروندان دولت‌ها ممکن است بر تصمیمات رهبران تأثیرگذار باشند، ولی اراده خصمانه رهبری است که باید تحت کنترل درآید.

بزرگ‌ترین کشفی که سبب ظهور عصر اطلاعات شد، آگاهی از این بود که هر چیزی در جهان خارج می‌تواند به ترکیبی از صفرها و یک‌ها کاهش یابد. این ترکیبات را می‌توان به‌صورت داده‌ها ازطریق الکترونیکی انتقال داد. برطبق کارهای صورت‌گرفته در زمینه کنترل نبرد ازسوی آرکیلا و رانفلت، اطلاعات چیزی بیش از محتوا یا معنای پیام است. در حقیقت، اطلاعات عبارت است از «هر تفاوتی که یک تفاوت را ایجاد می‌کند».[3] نبرد اطلاعاتی شکلی از

---

1. Richard Szafranski, "Toward a Theory of Neocortical Warfare: Pursuing the Acme of Skill," **Military Review**, Nov. 1994; and idem, "When Waves Collide: Conflict in the Next Century," **JFQ: Joint Force Quarterly**, Winter 1994-95.
2. Joseph A. Engelbrecht, "War Termination: Why Does a State Decide to Stop Fighting?", PhD diss., Columbia University, 1992. (Colonel Engelbrecht is a colleague at the Air University's Air War College).
3.Arquilla and Ronfeldt, note 9, p. 162.

بر طبق این تعریف، هر پیامی، بدون هیچ‌گونه «معنای» مشخص، هنوز «اطلاعات» محسوب می‌شود. این تعریف در زمانی‌که به بررسی تاکتیک‌های نبرد اطلاعاتی پرداخته می‌شود، سودمند است.

درگیری است که برای حمله به دانش یا اعتقادات حریف، به‌طور مستقیم به سیستم‌های اطلاعاتی آن حمله می‌کند و می‌توان آن را به‌عنوان جزئی از مجموعه‌ای بزرگ‌تر و جامع‌تر از فعالیت‌های خصمانه (جنگ شبکه‌ای یا جنگ سایبر) یا به‌صورت شکلی مجزا از فعالیتی خصمانه به‌کار برد.[1] اکثر تسلیحات (واژه‌ای که برای توصیف ابزارهای مهلک یا غیرمهلک نبرد به‌کار برده می‌شود) صرفاً در مقابل دشمنان خارجی سودمندی دارند؛ اما بسیاری از تسلیحات نبرد اطلاعاتی در مقابل دشمنان داخلی نیز مفید هستند؛ برای مثال، دولت یا گروهی خاص نمی‌تواند به‌صورت عادی از تفنگ و بمب برضد اعضای خود استفاده کند؛ درحالی‌که می‌تواند تسلیحات نبرد اطلاعاتی را به کار ببرد که البته تاکنون استفاده شده و در آینده نیز استفاده خواهد شد.

نبرد اطلاعاتی، فعالیتی خصمانه است که برضد هر بخش از سیستم‌های اطلاعاتی حریف جهت‌گیری شده است. «حریف» نیز کسی است که برطبق اهداف آن رهبر عمل نکند. به‌لحاظ خارجی این حریف را «دشمن» یا «غیرخودی» و به‌لحاظ داخلی، آن را «خائن»، «بزدل» یا «هوادار دشمن» (کسی که با رهبری که بر ابزارهای نبرد اطلاعاتی کنترل دارد مخالفت کرده یا همکاری زیادی ندارد) می‌نامند. اگر اعضای داخلی یک گروه در زمان نبرد حمایت چندانی از اهداف رهبر نداشته باشند، نبرد اطلاعاتی داخلی، ازجمله: تبلیغات، فریب، ترور شخصیت، شایعات و افتراها را می‌توان برای کسب حمایت بیشتر از اهداف رهبری مورد استفاده قرار داد.

۴. نبرد و ارتباط آن با آنچه می‌دانیم یا اعتقاد داریم

نبرد اطلاعاتی، برضد حریف خارجی یا داخلی، دارای این هدف نهایی است که با استفاده از تسلیحات اطلاعاتی، بر سیستم‌های دانش و اعتقادات حریف تأثیرگذار باشد؛ برای مثال، در یک نبرد، برای حریف خارجی سودمند است که بداند یا حداقل اعتقاد داشته باشد که دولت یا گروه مقابل در برابر او متحد است یا نه. نبرد اطلاعاتی سعی دارد تا به‌طور همزمان عوامل

1. Ibid

داخلی را به حمایت خود کشانده، حریفان خارجی را متقاعد سازد که دشمنش دارای جبهه‌ای متحد است و خواهان این است که این امر را در ذهن رهبری حریف جای دهد.

۴-۱. شکنندگی معلومات و اعتقادات

سیستم‌های معلومات، سیستم‌هایی هستند که برای حس و مشاهده شاخص‌ها و عوامل تعیین‌کننده، سازمان یافته و عمل می‌کنند. سپس این شاخص‌ها را به واقعیات قابل درک تبدیل کرده، این ادراکات را برای اتخاذ تصمیمات و هدایت اقدامات مورد استفاده قرار می‌دهند.[۱] زمانی‌که فردی حس می‌کند بشقابی داغ است، آن را رها می‌کند. زمانی‌که فردی مشاهده می‌کند هزینه‌هایش بیش از درآمدش است، مخارج خود را محدود می‌کند. سیستم‌های حسی و مشاهده‌ای ما این اجازه را می‌دهد تا از چیزی آگاهی یابیم. ما بر پایه معلومات خود تصمیم‌گیری و عمل می‌کنیم، ولی نه صرفاً برمبنای معلومات. سیستم‌های معلومات برطبق اصول علمی سازمان یافته‌اند و ازطریق روش علمی حفظ می‌شوند. به کلام‌دیگر سیستم‌های معلومات برای جمع‌آوری داده‌های تجربی ازطریق حس یا مشاهده، تدوین فرضیات، انجام آزمایشاتی که اعتبار یا عدم اعتبار فرضیات را مشخص می‌کند و استفاده از یافته‌ها به‌عنوان پایه‌ای برای اقدامات بیشتر در آینده، سازمان یافته‌اند. سیستم‌های اعتقادی، جهت‌گیری‌های آشکار و پنهانی هستند در برابر داده‌های تجربی در شکل ادراکات قابل اثبات و نیز در برابر دیگر داده‌ها و آگاهی‌هایی (کابوس‌ها، ترس‌ها، روان‌پریشی‌ها، روان‌رنجوری‌ها و دیگر چیزهایی که در باتلاق حاصلخیز ضمیر نیمه خودآگاه و ضمیر ناخودآگاه جمعی یا «روان‌پریشی ضمیر ناخودآگاه» وجود دارند)[۲] که قابل اثبات نیستند یا حداقل اینکه به آسانی

---

۱. پدیده‌شناختی را می‌توان به‌عنوان «تئوری پدیده‌های اساسی برای تمام معلومات تجربی» تعریف کرد.

Dorion Cairns, in Dagobert D. Runes, ed., **Dictionary of Philosophy**, Totowa, N.J.: Littlefield, Adams & Co., 1962, pp. 231-234.

2. C. G. Jung, **The Undiscovered Self**, New York: The New American Library, Mentor Book, 1958, p. 102.

ثابت نمی‌شوند.[1] به گفته جان بوید[2]، فرایند یا اقدام جهت‌گیری (آنچه بوید مشاهده، رویکرد، تصمیم‌گیری و اقدام می‌خواند) نیز تحت تأثیر میراث ژنتیکی و سنت‌های فرهنگی قرار دارد.[3] بنابراین جهت‌گیری رهبران آمریکا متفاوت از جهت‌گیری رهبران ژاپن یا چین، و جهت‌گیری کاپیتالیستی و رهبرانشان متفاوت از جهت‌گیری سوسیالیستی و رهبرانشان است.

برخلاف سیستم‌های معلومات، سیستم‌های اعتقادی بسیار شخصی و از فردی به فرد دیگر متفاوتند؛ علتش هم آن است که آنها دربردارنده مواد بسیاری از عناصر قدرتمند ضمیر ناخودآگاه و نیمه خودآگاهی هستند که دیگران و حتی خود فرد از آن آگاهی ندارند. اگرچه نبرد اطلاعاتی ذهن رهبری دشمن را هدف قرار می‌دهد، ساده‌انگارانه خواهد بود اگر تصور کنیم دشمن «یک ذهن» است. درحقیقت، دشمن متشکل از اشخاص بسیار با اذهان بسیار است. این امر مسئله را کمی پیچیده می‌سازد؛ برای مثال، اگر دشمن دارای اذهان پراکنده و مجزایی است، آیا می‌توان به‌صورت مجزا به آن حمله کرد؟ اگر دشمن متمرکز باشد (بیش از نیمی از مردم جهان تا سال ۲۰۲۰ در مجموعه شهرهای بزرگ زندگی خواهند کرد و به‌واسطه تکنولوژی اطلاعات در شمار بسیار قابل دسترس خواهند بود)، حمله را می‌توان برضد گروه‌های بزرگ انجام داد. بدین‌ترتیب هدف نبرد عبارت است از کنترل اراده خصمانه رهبران و تصمیم‌گیرندگان حریف. این امر را می‌توان به‌طور مستقیم ازطریق حملاتی با هدف تأثیرگذاری یا دست‌کاری معلومات و اعتقادات رهبر حریف یا به‌طور غیرمستقیم با حمله به معلومات یا اعتقادات کسانی که رهبر برای اقدام به آنها وابسته است، انجام داد. معمولاً شناسایی رهبران و تصمیم‌گیرندگان در سلسله مراتب هر سازمان مشکل نیست. زمانی‌که

---

۱. نبرد اطلاعاتی نیازمند آن است که فلاسفه، مردم‌شناسان فرهنگی، متخصصان مناطق، زبان‌شناسان و معناشناسان به ستاد «عملیات‌ها» ملحق شوند. هم‌اکنون روزهایی که دانشکده‌های جنگ یا دانشکده‌های ستاد این رشته‌ها را مورد غفلت قرار می‌دادند، سپری شده است.

2. John Boyd

3. John R. Boyd, briefing slides, subject: A Discourse On Winning and Losing, August 1987. Maxwell AFB, Alabama.

سازمانی قدرت یا زور را اعمال می‌کند، دارای ویژگی سلسله مراتبی است. بنابراین معلومات و اعتقادات تصمیم‌گیرندگان، پاشنه آشیل (نقطه ضعف) این سازمان‌های سلسله مراتبی هستند.

ازآنجایی‌که سیستم‌های معلوماتی علمی‌ترند، به نسبت سیستم‌های اعتقادی کمتر تحت تأثیر فرهنگ یا عوامل غیرعقلانی و غیرقابل اثبات قرار می‌گیرند. باوجوداین هر دو سیستم معلوماتی و اعتقادی اجزایی هستند که در سیستم تصمیم‌گیری بشری وجود دارند.[1] آنچه شناخته می‌شود، ازجمله روش‌های کسب شناخت را می‌توان ازطریق رابطه آن با چیز دیگری مورد آزمایش قرار داد و اعتبار یا عدم اعتبار، درستی یا نادرستی و واقعی یا غیرواقعی بودن را تعیین کرد. همه آن چیزها که بدانها اعتقاد پیدا می‌کنیم، تحت همان آزمایش‌ها قرار نمی‌گیرند. به‌همین‌صورت حالت اجبارکنندگی اعتقادات کمتر از شناخت تجربی نیست. معلومات و اعتقادات هر دو بر تصمیم‌گیری بشری تأثیرگذار هستند. ازآنجایی‌که هدف نبرد عبارت است از: تأثیرگذاری بر رفتار حریف ازطریق نفوذ بر تصمیمات آن، اقدامات نبرد اطلاعاتی باید برضد هر دو سیستم معلوماتی و اعتقادی حریف جهت‌گیری شوند. اگر حریف به‌صورت ائتلافی از مراکز متعدد باشند، بسیاری از سیستم‌های اعتقادی ممکن است در این ائتلاف وجود داشته باشند. این امر ممکن است سبب شکست آن گردد؛ ازاین‌رو ائتلاف نباید از دولت‌ها یا گروه‌های جداگانه‌ای تشکیل شده باشد که به‌صورت اتحاد عمل می‌کنند. ائتلاف می‌تواند در یک دولت یا داخل گروه‌هایی صورت گیرد.

۴-۲. هدف قراردادن شناخت‌شناسی[2]

سیستم مورد هدف نبرد اطلاعاتی می‌تواند دربردارنده هر عنصری در شناخت‌شناسی حریف باشد. شناخت‌شناسی به‌معنای «سازمان، ساختار، روش‌ها و اعتبار معلومات» است[3] و در اصطلاح عامیانه یعنی هر چیزی که ارگانیسم بشری (فردی یا گروهی) آن را صحیح یا واقعی

---

1 Ibid.
2. Epistemology
3. Ledger Wood, in Runes, pp. 94-96.

می‌داند، بدون توجه به اینکه آن چیز جزء معلومات باشد یا اعتقادات. در سطح استراتژیک، هدف از یک نبرد اطلاعاتی کامل عبارت است از: تأثیرگذاری بر انتخاب‌های حریف؛ لذا رفتار حریف بدون آگاهی او از انتخاب‌ها و رفتارش، تحت تأثیر قرار می‌گیرد. اگرچه دستیابی به این هدف مشکل است، همچنان هدف نبرد اطلاعاتی کامل در سطح استراتژیک است. یک نبرد اطلاعاتی موفق (نه لزوماً کامل) در سطح استراتژیک به تصمیماتی ازسوی حریف منتج می‌شود که با نیات و اهداف رهبر حریف همخوانی ندارد.

نبرد اطلاعاتی موفق در سطح عملیاتی با تأثیرگذاری بر توانایی اتخاذ تصمیمات به‌موقع و کارآمد، پشتیبان اهداف استراتژیک خواهد بود. به‌کلام‌دیگر هدف از فعالیت‌های نبرد اطلاعاتی در سطح عملیاتی عبارت است از: پیچیده کردن و محدود ساختن فرایند تصمیم‌گیری حریف، به‌گونه‌ای که نتواند به شیوه‌ای مؤثر و هماهنگ اقدام کند. در نبرد اطلاعاتی، هدف عبارت است از: هماهنگ ساختن فعالیت‌های اتخاذشده در سطح عملیاتی با فعالیت‌های سطح استراتژیک، به‌گونه‌ای که حریف تصمیماتی را اتخاذ کند که در راستای اهداف ما باشد.

در سطح استراتژیک، رهبرانی که نبرد اطلاعاتی را در ذهن خود دارند، باید حداقل پاسخ سه سؤال را بدانند: اول آنکه، رابطه نبرد اطلاعاتی با اهداف گسترده‌تر آن چیست؟ دوم آنکه، وقتی نبرد اطلاعاتی به نتیجه رسید، می‌خواهیم که رهبران حریف چه معلومات و اعتقاداتی داشته باشند؟ یعنی اینکه وضعیت شناخت‌شناسی مطلوب و درنتیجه معیار موفقیت چیست؟ سوم آنکه، بهترین ابزارهای نبرد اطلاعاتی برای رسیدن به معیارهای موفقیت چیست؟ یعنی «ابزارها» چگونه با «اهداف» ارتباط پیدا می‌کنند؟

در سطح عملیاتی، رهبران مسئول اجرای «تاکتیک‌های برتر» نیز باید پاسخ برخی سؤالات را بدانند. آیا اهداف یا تسلیحات ممنوعه‌ای در حملات نبرد اطلاعاتی وجود دارد؟ آیا وضعیت نهایی شناخت‌شناسی در هرکجا و هرزمانی به‌دست می‌آیند یا اینکه وضعیت‌های موقتی وجود دارند که باید در حوزه‌های جغرافیایی، زمان یا بخش‌های مشخصی از فعالیت اطلاعاتی

به‌دست آیند؟ مسائل «فرماندهی و علامت»[1] نیز باید مورد توجه قرار گیرد. مهم‌تر اینکه، رهبران در سطح عملیاتی باید بدانند که حملات در چه زمانی پایان خواهند یافت و چه وسایلی برای انتقال فرمان پایان حمله مورد استفاده قرار خواهند گرفت. این مسائل بسیار مهم هستند؛ زیرا تسلیحات اطلاعاتی، متناسب با تسلیحات مورد استفاده، می‌توانند خسارات جانبی زیادی نیز به سیستم‌های معلومات و اعتقادی حمله‌کننده وارد کنند.[2] در بدترین حالت، واکنش حریف می‌تواند ضد حملاتی علیه سیستم‌های اطلاعاتی «خودی» باشد که تا حدی از خسارات جانبی به‌وجود آمده از تشابه اطلاعاتی «آتش خودی» قابل تمایز نیست. این امر نیازمند بررسی بیشتری است.

نبرد، یک فعالیت اجتماعی بشری است[3] و صحنه عمل مبارزان، جامعه است، متشکل از کسانی که درگیر نبرد بوده‌اند و گروه‌های فعال و منفعل. ازآنجایی‌که نبردها به کنش، واکنش و تعامل بشری بستگی دارند، نتایج برخی از آنها غیرقابل پیش‌بینی است. همانطورکه گرانت هاموند[4] در «معضلات جنگ» عنوان می‌دارد، اگر نتایج جنگ را از پیش می‌دانستیم، آنگاه بازنده آن دلیلی برای جنگیدن نداشت.[5] به‌علاوه ممکن است فواصلی زمانی میان کنش و واکنش وجود داشته باشد؛ برخی نتایج دیرتر از نتایج دیگر به‌ثمر می‌رسند؛ ازاین‌رو این ایده

---

1. Command and Signal

۲. تأثیراتی که من به آنها اشاره می‌کنم، پیچیده‌تر از ناتوانی برای جلوگیری از مداخله گرفتاریتان در سیستم‌های ارتباطی شماست. این تأثیرات غیرقابل مهار و گسترش‌یابنده را می‌توان مدل‌سازی نمود و تا حدودی تأثیرات آنها را جبران کرد. تسلیحات و تأثیرات نبرد اطلاعاتی به‌آسانی قابل کنترل و مهارپذیر نیستند. در نبرد معمول است که دشمن را بد جلوه داده، مورد تمسخر قرار دهند که این امر معمولاً شکل جوک به خود می‌گیرد. اگر هدف این جوک‌ها گروه قومی خاصی باشد، رسماً به‌عنوان جوک‌های نژادی شایع می‌شوند. اگر گروه قومی بخشی از شهروندان خودی باشد، چنین حملاتی می‌تواند زیان‌ها و خسارات جانبی به همراه داشته باشد. خسارات جانبی به نیروهای مسلح ممکن است تأثیراتی نظیر: ظهور نژادپرستی را سبب شود. اگر کسی بپذیرد که تسلیحات و حملات دارای تأثیرات احتمالی است، آنگاه برخی نتایج غیرقابل پیش‌بینی خواهند بود.

3. Martin VanCreveld, op.cit., p.35. 4. Grant Hammond.

5. Grant T. Hammond, "Paradoxes of War," **JFQ: Joint Forces Quarterly**, Spring 1994.

که جنگ جهانی دوم نتیجه جنگ جهانی اول (یا معاهده صلحی که به این جنگ خاتمه داد) بود، ممکن است صحیح باشد. به‌هرحال پیش‌بینی‌ناپذیری به نتایج و پیامدهای خاتمه جنگ محدود نمی‌شود. اقدامات و کنش‌های مشخص در نبرد می‌توانند واکنش‌های مشخص و غیرقابل پیش‌بینی را به همراه داشته باشد.

حملات اطلاعاتی ـ که سیستم‌های معلوماتی یا اعتقادی حریفان را هدف قرار می‌دهند ـ می‌توانند پیامدهایی داشته باشند که به‌اندازه حملات نظامی با هدف تخریب و نابودی فیزیکی اصول یا تجهیزات نظامی دشمن یا کشتار موجودات بشری غیرقابل پیش‌بینی باشند. ذکر این نکته کافی است که حملات اطلاعاتی دارای تأثیرات و پیامدهای احتمالی هستند و اگر از پیش مورد توجه و ارزیابی قرار نگیرند، به نتایج دلخواه نخواهند رسید. بدتر اینکه، ممکن است آنچنان پیامدهای نامطلوبی داشته باشند که حمله‌کننده از اقدام خود پشیمان شده، افسوس بخورد. ایده پیامدهای احتمالی، همچون ایده خسارات جانبی، نیازمند بررسی و توجه در سطوح استراتژیک و عملیاتی نبرد اطلاعاتی است.

۴-۳. مجموعه‌هایی که در نبرد اطلاعاتی مورد هدف هستند

حریف برای تصمیم‌گیری بیش از همه بر سیستم‌های اطلاعاتی وابسته است و دست‌کاری خصمانه این سیستم‌ها نیز بیشترین آسیب‌پذیری را برای او به همراه دارد؛ برای مثال، ویروس‌های نرم‌افزاری تنها به کسانی صدمه می‌زنند که به آن نرم‌افزار وابسته هستند.

اگرچه این امر بیانگر آن است که تنها دولت‌ها یا سازمان‌ها و گروه‌های پیشرفته (اطلاعات پایه) در برابر نبرد اطلاعاتی آسیب‌پذیرند، عکس این موضوع هم می‌تواند صادق باشد؛ زیرا عامه مردم، سازمان‌ها و گروه‌های مبتنی‌بر کسب‌وکار سنتی نیز هنوز دارای سیستم‌های هستی‌شناختی آسیب‌پذیر هستند. ازآنجایی‌که نبرد اطلاعاتی را می‌توان برضد کل هستی‌شناسی حریف (سیستم‌های معلوماتی و سیستم‌های اعتقادی) به‌کار برد، این جمعیت‌ها نیز در برابر نبرد اطلاعاتی آسیب‌پذیر هستند.

دراین‌خصوص می‌توان از مقایسه مالک و معمار مثال زد. مالک ممکن است از نواقص محل سکونت خود آگاه نباشد، ولی معمار آگاه است. به‌همین‌صورت عامل یا «مالک» یک سیستم رتباطاتی که توسط دیگران ساخته شده، ممکن است از ویژگی‌ها و جنبه‌های مهم آن ـ که فقط طراح و سازنده از آن آگاهی دارند ـ مطلع نباشد. اگر معمار در برابر «مالک» به‌طور مستقیم تابع یا مسئول نباشد، آنگاه این احتمال وجود دارد که معمار از جنبه‌های پنهان به‌نفع خود سوءاستفاده کند. در نبرد رقابت تجاری، معمار انگیزه، وسایل و فرصت سوءاستفاده از این جنبه‌ها را برای رسیدن به اهداف خود داراست، خواه دولت یا حکومت اقدامات او را تأیید کند یا نه.

در مورد جوامع یا گروه‌های پیشرفته، حملات برضد سیستم‌های اطلاعاتی می‌توانند ضربه جبران‌ناپذیری بر توانایی تصمیم‌گیری حریف در نبرد وارد سازند. باوجوداین باید در نظر داشت که می‌توان از هر چیزی، حتی یک پدیده طبیعی، نظیر: کسوف، در حمله به سیستم‌های اعتقادی یک گروه کمترپیشرفته استفاده کرد. توتم‌ها و تابوها نیز ممکن است اهداف یا ابزارهای نبرد اطلاعاتی برضد یک گروه ابتدایی باشند. بنابراین، آسیب‌پذیری در مقابل نبرد اطلاعاتی تقریباً جهانی است و تنها میزان آن متفاوت است.

۴-۴. نمایی از پیچیدگی نبرد اطلاعاتی

نبرد اطلاعاتی، ایده‌ای پیچیده است؛ زیرا تسلیحات به‌کار گرفته شده در آن، واژه‌ها و تصاویر هستند. در این نوع نبرد، حملات توسط اذهان برای تأثیرگذاری بر اذهان طرح‌ریزی می‌شوند و آنها را می‌توان به‌صورت مستقیم یا غیرمستقیم برضد اهداف خارجی و داخلی نشانه‌گیری کرد. پیامد و نتیجه مطلوب نبرد اطلاعاتی نیز عبارت است از: تأثیرگذاری و تغییر اعتقادات و معلومات حریف.

به‌طورمثال شورشی در هند (۵۷-۱۸۵۸) با این شایعه آغاز شد که بریتانیا فشنگ اسلحه‌ها را با روغن حیوانی پوشش می‌دهد.[1] تماس با این روغن برای هندوها حرام بود. اگرچه پوشش

1. George C. Kohn, **Dictionary of Wars**, New York: Facts On File Publications, 1986, p. 214.

فشنگ‌ها از روغن حیوانی نبود و می‌توانست با آزمایش‌های علمی ثابت شود، آنان اعتقاد داشتند که این ماده روغن حیوانی است. این اعتقاد، بیش از دانش برگرفته از آزمایش‌های علمی برای آنها اهمیت داشت. بنابراین، اعتقاد و نه دانش یا معلومات بر رفتار هندوها تأثیر گذاشت و درگیری سختی را میان بریتانیا و آنها موجب شد. این مثال همچنین نشان‌دهنده این حقیقت است که اگرچه استفاده از این اطلاعات غلط برضد رهبری بریتانیا جهت‌گیری شده بود، حمله‌ای غیرمستقیم محسوب می‌شد. رهبران هندوها این شایعه را پراکنده ساختند و دراین‌خصوص سیستم‌های اعتقادی هندی‌ها را برای شورش بر ضد اربابان بریتانیایی خود، مورد حمله قرار دادند.

بنابراین نبرد اطلاعاتی را می‌توان توسط جوامع یا گروه‌های مختلف با توانایی‌های متفاوت اقتصادی و تکنولوژیکی و نیز برضد یا میان آنها ازنظر داخلی یا خارجی به‌کار برد.[1] زمانی‌که این نبرد علیه حریفان داخلی باشد، هدف آن استفاده از این حریفان برای رسیدن به هدف والاتر نبرد است، مانند: کنترل اراده خصمانه حریف خارجی، و زمانی‌که نبرد اطلاعاتی در مقابل حریفان خارجی باشد، هدف کنترل اراده خصمانه رهبران حریف خارجی خواهد بود.[2]

۴-۵. آسیب‌پذیری پیچیده؟

در دولت‌ها یا گروه‌هایی با توانایی بالای تکنولوژیکی و اقتصادی، مجموعه‌هایی که در سطوح استراتژیک مورد هدف نبرد اطلاعاتی قرار می‌گیرند، بسیار ارزشمند هستند؛ نظیر: سیستم‌های

---

۱. اقتصادی ـ تکنولوژیک واژه‌ای است که توسط جوزف ای. انگلبرت به‌کار برده شد. وی آن را «مربوط به پیشرفت در توسعه کاربرد اصل علمی (تکنولوژی)، ثروت (اقتصاد) و رابطه میان پیشرفت در علم و افزایش ثروت اقتصادی» می‌داند.

2. Gerald R. Hurst, "Taking down Telecommunications", Thesis, School of Advanced Airpower Studies, Air University, Maxwell Air Force Base, Ala., 28 May 1993.

ارتباطات و تلفن[1]، حسگرهای فضایی، تقویت ارتباطات؛ کمک‌های ماشینی و خودکار به تعاملات مالی، بانکداری و تجاری؛ سیستم‌های تولید و توزیع قدرت؛ سیستم‌های فرهنگی از همه نوع و کل طیف سخت‌افزاری و نرم‌افزاری که چگونگی معلومات و اعتقادات دشمن را نشان می‌دهد. همچنین سیستم‌های اطلاعاتی استراتژیک در دولت‌هایی با توانایی بالای اقتصادی ـ تکنولوژیک که اغلب در سطوح عملیاتی از پیچیدگی زیادی برخوردار هستند، همگی در برابر حمله آسیب‌پذیرند.

تازمانی‌که خصومت‌ها آشکار نشده‌اند، باید از نبرد اطلاعاتی بهره برد. رهبری حریف وقتی به یک یا چند مورد زیر اعتقاد پیدا کند، احتمال کمتری دارد که به جنگ روی آورد: خشونت بد است، بدون متحد خواهد ماند، با تحریم‌های شدیدی روبه‌رو خواهد شد، زیرساخت‌های صنعتی آن از نبردی طولانی‌مدت حمایت نخواهند کرد یا اینکه نیروهای مسلح آن آماده نیستند. اگر نبرد واقعی آغاز شود، حملات در سطح عملیاتی می‌توانند با حملات در سطوح استراتژیک هماهنگ گردند.

اهداف در سطح عملیاتی نیز وقتی حریف دارای توانایی بالای اقتصادی ـ تکنولوژیک بوده و بر کمک‌های ماشینی و خودکار برای جنگیدن متکی است، سودمند خواهند بود. سیستم‌های سلسله مراتبی بیشترین آسیب‌پذیری را دارند، ولی حتی شبکه‌ها نیز دارای کنترل بوده یا نقاطی را تقویت می‌کنند که برای حمله مناسب است. شبکه‌ها برای عملکرد صحیح و کارآمد نیز دارای عناصری سلسله مراتبی هستند. اغلب این عناصر نامرئی‌اند (پروتکل‌های نرم‌افزاری، فیلترها، دستورات، دسته‌بندی و مشابه آن). اینکه حمله به آنها مشکل است به‌معنای مصونیت آنان در برابر حملات نیست.

هرچه دولت‌ها یا گروه‌ها از سطح بالای توانایی‌های اقتصادی ـ تکنولوژیک برخوردار بوده، تعاملات بیشتری با دیگر گروه‌ها (ازجمله گروه‌های داخلی) یا دولت‌ها داشته باشند،

---

1. Ibid.

به‌همان نسبت نیز آسیب‌پذیریشان در نبرد اطلاعاتی بیشتر خواهد بود. زمانی‌که اندازه شبکه افزایش می‌یابد، ممکن است آسیب‌پذیری نیز افزایش یابد که البته به افزایش تعامل اطلاعات یا میزان و حجم افزایش تعاملات بستگی دارد. درنتیجه دولت یا گروهی که در سطح جهانی به تعامل می‌پردازد، در همان سطح نیز دارای آسیب‌پذیری است (اگر هدف از این تعامل، نبردی استراتژیک با هدف تأثیرگذاری بر معلومات یا اعتقادات دیگران باشد، آنگاه دیگران نیز که به تعامل می‌پردازند، دارای آسیب‌پذیری مشابهی خواهند بود). دموکراسی‌ها آسیب‌پذیری کمتری نسبت به رژیم‌های خودکامه ندارند، اگرچه سیستم‌های سوسیال دموکراتیک از تساهل بیشتری برخوردار هستند. این بدان معناست که دموکراسی‌ها تنوع را ترویج داده و تنوع نیز تساهل را برای تفاوت افزایش می‌دهد. این تمایل برای پذیرش تنوع و گوناگونی، همزیستی معلومات و اعتقادات متناقض و متفاوت در میان اشخاص و گروه‌ها و تلاش دائمی برای کنترل ازسوی متخصصان، آسیب‌پذیری دموکراسی را کاهش نمی‌دهد، ولی تأثیر حملات نبرد اطلاعاتی را کم می‌کند. به‌کلام دیگر بسیاری از مردم کشورهای دموکراتیک ممکن است در برابر این حملات مصون باشند؛ زیرا معلومات آنها محدود و سیستم‌های اعتقادیشان انعطاف‌پذیر بوده، اطلاعات زیاد را صرفاً به‌عنوان جاروجنجال در نظر می‌گیرند. بنابراین، تصاویر شهوت‌انگیز در تلویزیون، تأثیر اندکی بر بسیاری از مردم ایالات متحده دارد؛ اما اگر همان تصاویر در چین، عراق یا ایران پخش شود، می‌تواند تأثیرات بسیار زیادی داشته باشد.[1]

---

۱. ایران مثال خوبی است. تحقیقات مجلس از سازمان صداوسیما بیانگر حساسیت این کشور نسبت به محتوا و معنای پیام‌های تصویری است. به این اظهارات که در تحقیقات مجلس آمده توجه کنید:

«رهبر جمهوری اسلامی بارها به سازمان صداوسیما و مدیر آن توصیه کرده و دستور داده؛ اما متأسفانه، دستورات و نظر ایشان به اجرا در نیامده است. برای مثال... از سال ۱۳۶۸ تا ۱۳۷۰، ایشان چهارده بار به این سازمان مطالبی را یادآور شده‌اند که عبارت است از: الف. ارائه اطلاعات نادرست، ب. سطح پایین کیفیت برنامه‌های برون‌مرزی و ناتوانی در تبلیغ و گسترش دیدگاه‌های اسلامی در آن، ج. پخش جملات کفرآمیز در مورد پرهیزگاری، د. نشان دادن اشخاص در نقش امامان معصوم».

اگرچه سیستم سوسیال دموکراتیک دارای تساهل است، دستگاه کنترل اقتصادی - تکنولوژیک آن کمتر این‌گونه است. هم‌اکنون سیستم‌های بانکداری، مالی، تجاری و مسافرتی و کنترل ترافیک هوایی وابستگی بیشتری به سیستم‌های تکنولوژی اطلاعات پیدا کرده‌اند. در سال ۱۹۹۲ ایالات متحده بیش از ۲۱۰ میلیارد دلار در تکنولوژی اطلاعاتی سرمایه‌گذاری کرد (در حدود نیمی از کل سرمایه‌گذاری‌ها در سطح جهان) و انتظار می‌رود که این میزان در هر سال با هجده درصد افزایش مواجه باشد.[۱] با افزایش وابستگی به سیستم‌های اطلاعاتی، نبرد ازسوی گروه‌های غیردولتی (تروریست‌ها، افراط‌گرایان مذهبی) برضد سیستم‌های اطلاعاتی به تهدیدی واقعی تبدیل شده است. حمله به مرکز تجارت جهانی با هر هدفی، آشکار بود که برای ضربه زدن به توانایی تجاری و بانکداری ایالات‌متحده انجام شده بود. نبرد اطلاعاتی تروریست‌ها در آینده به‌طور قطع تأسیسات تولید قدرت و سیستم‌های ارتباطاتی را مدنظر خواهد داشت. حملات همزمان به نقاط مختلف نیز می‌توانند تأثیر استراتژیک داشته باشند؛ بدین‌معنا که بر معلومات، اعتقادات و اراده رهبران تأثیرگذار باشند.

نکته هشداردهنده آن است که چون نبرد اطلاعاتی در سطح استراتژیک بر این هدف استوار است که اراده خصمانه حریف را با تأثیرگذاری بر معلومات و اعتقادات آن تحت کنترل خود درآورد، نمی‌توان میان مبارزان و غیرمبارزان تمایزی را مشاهده کرد. ازآنجایی‌که تسلیحات نبرد اطلاعاتی به‌لحاظ نظام‌مندی، سیستم‌های معلوماتی و اعتقاداتی حریف را مورد حمله قرار می‌دهند، قبل از آنکه حملات اطلاعاتی صورت گیرد، باید نتایج احتمالی نبرد اطلاعاتی را به‌دقت مورد ارزیابی قرار داد. یک نبرد اطلاعاتی موفق اطلاعات فریب را بر روی هدف بشری، جایگزین اطلاعات واقعی می‌نماید. در سطح استراتژیک، این اهداف شامل مبارزان و

... عربستان سعودی نیز به‌تازگی در غیرقانونی کردن استفاده از گیرنده‌های ماهواره به چین ملحق شده است. دراین‌خصوص می‌توان به‌آسانی تأثیرات شبکه موزیک تلویزیون (MTV) را بر چنین فرهنگ‌هایی مشاهده کرد.

۱. یکی از مجریان ارتباطات که در اجلاس دانشگاه هوایی سخنرانی می‌کرد، به شرط عدم ذکر نامش این ارقام را فاش نموده است.

غیرمبارزان می‌شود.

فریب و دروغ‌پراکنی، نبرد الکترونیک، تبلیغات و کل طیف «نبرد روانی» یا حملات نبرد فرماندهی و کنترل برضد مبارزان دشمن در سطح عملیاتی ازجمله اقدامات مناسب در نبرد اطلاعات است. این اقدامات با هدف کنترل دشمن بدون جنگ یا کاهش میزان خشونت صورت می‌گیرد. فریب خوردن و دور شدن از واقعیت در یک نبرد، همانند کشته شدن یا جراحات در جنگ، خطری است که مبارزان از آن آگاهی دارند و احتمالی است که باید آن را بپذیرند. بنابراین، تازمانی‌که نبرد اطلاعاتی و تسلیحات آن به‌واسطه هنجارها یا قوانین به سطح عملیاتی محدود شده‌اند، نمی‌توان آنها را نسبت به دیگر تسلیحات شیطانی و ناعادلانه دانست. مشکل همچنان دارای دو جنبه است: تعیین اخلاقیات نبرد اطلاعاتی که در سطح استراتژیک صورت می‌گیرد و محدود کردن استفاده از تسیلحات اطلاعاتی به سطح عملیاتی.

۵. کارکردهای نبرد اطلاعات

نبرد اطلاعاتی[1] در مفهومی عام و گسترده عبارت است از: استفاده اطلاعاتی جهت رسیدن به اهداف ملی. این مفهوم همانند دیپلماسی، توانمندی رقابت اقتصادی یا استفاده از نیروی نظامی، نقش کلیدی در قدرت ملی ایفا می‌کند و مهم‌تر از همه اینکه به‌تدریج به یک منبع ملی حیاتی برای حمایت از دیپلماسی، توانمندی رقابت اقتصادی و به‌کارگیری مؤثر قدرت نظامی تبدیل می‌شود. نبرد اطلاعاتی را می‌توان به‌عنوان مناقشه‌ای مداوم در سطح جامعه‌شناختی وسیع یا سطح ملی در برابر دیگران تعریف کرد؛ زیرا اینک شبکه‌ای جهان‌گستر در زمینه اطلاعات و ارتباطات ایجاد شده است.[2] آنچه در این مفهوم از نبرد اطلاعات مطرح می‌شود ـ که درعین‌حال بسیار مهم نیز هست ـ ظهور «مهاجم» است. به احتمال زیاد در آینده، ملت‌ها در

---

1. Information Warfare
2. John Arquilla and David Ronfeldt, “Cyberwar is Coming!” **Comparative Strategy,** No. 12 Apr.-June 1993, PP. 141-165.

سطح استراتژیک به مقابله با یکدیگر خواهند پرداخت. همچنین نبرد اطلاعاتی در روش مهاجمان یا حتی در سطح فعالیت‌های جنگی و فعالیت‌های روزمره نظامی تغییر ایجاد خواهد کرد و در نهایت می‌تواند باعث شود تا یک مهاجم «فعالیت‌هایی بیش از جنگ» انجام دهد؛ لذا نقطه‌ای کانونی در تفکر جنگی آینده خواهد بود.

نبرد اطلاعاتی اساساً درباره ایده‌ها و هستی‌شناختی است. بنابراین به روش تفکر انسان‌ها و مهم‌تر از آن، روش تصمیم‌گیری انسانی مربوط می‌شود و اگرچه حوزه فعالیت آن می‌تواند وسیع باشد، صرفاً هدفش شبکه‌های ارتباطی[1] یک جامعه یا بخش نظامی آن، پرداختن به ماهواره‌ها، امواج رادیویی یا رایانه‌ها نیست، بلکه به‌دنبال اعمال نفوذ بر انسان‌ها و تصمیم‌گیری‌هایشان است. بزرگ‌ترین تهدید علیه بخش‌های اطلاعاتی این است که این بخش‌ها در تفکر نسبت به این مفهوم تسلیم وسوسه پذیرش تکنولوژی‌های جدید، به‌ویژه تکنولوژی‌های اطلاعاتی[2] شوند، بدون اینکه به سایر ابعاد مسئله توجه کنند[3] این، اشتباه استراتژیک تاریخی است که صرفاً به تکنولوژی نظامی اتکا شود. توانمندی تکنولوژی‌های نبرد اطلاعاتی می‌تواند گسترده، دقیق و مهلک باشد و امکان دید و فرصت مناسب برای انقلاب نظامی را بگیرد. نبرد اطلاعاتی، نبردی حقیقی است؛ لذا هدف این جنگ، ایجاد عدم توازن میان دو رقیب است و آنگونه‌که سان تزو می‌گوید، وادار ساختن رقیب به شکست است، پیش از اینکه بتواند از نیروهایش استفاده و یا تیرهایش را پرتاب کند.

بنابراین هدف نبرد اطلاعاتی تأثیرگذاری بر افکار و به‌ویژه افکاری است که تصمیمات کلیدی جنگ و صلح را می‌گیرند و نیز از منظر نظامی، افکاری که در ساختار استراتژی نظامی به تصمیمات کلیدی در مورد زمان و نحوه به‌کارگیری امکانات و توانمندی‌های نظامی می‌پردازند. براین‌اساس توانمندی‌های اخیر ایجادشده در فعالیت‌های روانشناسی، مسائل

---

1. Communication Networks 2. Information Technology

3. Carl H. Builder, **The Icarus Syndrome: The Role of Air Power Theory in the Evolution and State of the U.S. Air Force**, New Brunswick, N.J.: Transaction Publishers, 1994.

عمومی و مدنی به‌همراه آژانس‌های اطلاعاتی، طراحان ماهواره‌ای[1]، متخصصان ارتباطات[2] و نوابغ کامپیوتر[3] بیانگر توسعه در عرصه نبرد اطلاعات هستند.[4] درحالی‌که مفهوم نبرد اطلاعاتی دربرگیرنده کامپیوترها، جنگ الکترونیک و شبکه‌های ارتباطی در فعالیت‌های نظامی بوده، مناقشات میان‌دولتی را تحت تأثیر خود قرار می‌دهد، مجموعه‌ای از بازیگران جدید و خطرناک در فضای سایبر نیز وارد عرصه نبرد اطلاعات می‌شوند. چنین بازیگرانی درحال افزایش هستند و می‌توانند شامل عوامل سیاسی غیردولتی نظیر: صلح سبز، عفو بین‌الملل[5]، هکرهای کامپیوتری یا تروریست‌ها باشند.

ازسوی‌دیگر نبرد اطلاعاتی را به‌سادگی می‌توان استفاده از اطلاعات برای رسیدن به اهداف ملی تعریف کرد که همانند ارتش‌های رسمی، سیاست، اقتصاد و دیگر نهادهای ملی برای تأمین اهداف ملی در تلاش است. برای جلوگیری از سوءتفاهم، تعریف فوق را می‌توان به دو بخش مجزای: جنگ رایانه‌ای[6] و جنگ شبکه‌ای[7] تقسیم‌بندی کرد.

ماهیت نبرد اطلاعاتی بر انگاره‌ها و شناخت‌شناسی از جنگ تأثیر می‌گذارد. شناخت‌شناسی در اینجا به معنای روشی است که انسان‌ها تفکر و تصمیم‌گیری می‌کنند. لذا می‌توان دریافت که ایده نبرد اطلاعاتی منحصراً وابسته به وجود شبکه‌های انتقال داده‌ها مانند: ماهواره‌ها، سیستم‌های کامپیوتری و مخابراتی نیست، بلکه بیشتر بر جنبه روانی و فرماندهی استراتژیک جنگ تأثیر دارد. امروزه در تمامی کشورهای جهان تکنولوژی و زیرساخت ایجاد سیستم فرماندهی براساس اصول جنگ‌های رایانه‌ای تا حد مطلوبی فراهم است؛ ولی پیاده‌سازی این اصول بستگی به تصمیمات رده‌های بالای مملکتی دارد.

درصورت تصمیم به ایجاد سیستم جنگ رایانه‌ای در یک کشور، ابتدا لازم است با

---

1. Satellite Drivers
2. Communications Specialists
3. Computer Wizards
4. "Information Dominance Edges toward New Conflict Frontier," **Signal**, No. 48, Aug. 1994, PP. 37-39.
5. Amnesty International
6. Cyber War
7. Net War

تمرکززدایی[1] از سیستم فرماندهی، صدور دستورات عملی را به مراکز نظامی کوچک‌تر که به‌طور مستقیم در مناطق جنگی حضور دارند واگذار کرد و سپس با گسترش زیربنای اطلاعاتی موجود ازطریق ایجاد شبکه‌هایی با اشکال غیرقابل انقطاع، امکان دسترسی این مراکز به بانک‌های اطلاعاتی جنگی کشور را به‌منظور اتخاذ بهترین تصمیم فراهم نمود. در نهایت امر نیز لازم است اطلاعات جمع‌آوری‌شده از مراکز مختلف (خودی و غیرخودی) را ازطریق شبکه‌های مخابراتی به مرکز فرماندهی کل کشور انتقال داد تا در آنجا کارشناسان جنگ (که دیگر نیاز نیست الزاماً نظامی باشند) با استفاده از اطلاعاتی که متخصصان تحلیل داده‌های کامپیوتری در اختیار آنها می‌گذارند، هدف‌های عمومی را به‌دست آورده، به مراکز کوچک‌تر اعلام کنند. ازطرف‌دیگر، نبرد اطلاعاتی شامل جنگ شبکه‌ای نیز می‌شود. این جنگ با تعاریف معمول جنگ تفاوت داشته و به‌طور دائم باید با حمایت غیرعلنی دولت‌ها با دو هدف جریان داشته باشد:

۱. به‌دست آوردن اطلاعات از فعالیت‌ها، موجودی‌ها و تصمیمات دولت‌های دیگر؛

۲. جلوگیری از دسترسی دشمن به اطلاعات خودی ازطریق تقویت سیستم‌های دفاعی موجود در شبکه. در این جنگ، میدان نبرد امواج ماهواره‌ای و اینترنت است. کشورها برای آنکه اطلاعات خود را در تمامی کشور قابل استفاده سازند، به اجبار، آن را روی اینترنت قرار می‌دهند و درنتیجه متخصصان کامپیوتری کشورهای دیگر خواهند توانست ازطریق نفوذ در شبکه‌ها به آن دسترسی پیدا کنند. جنگ امروز، جنگ برای حفظ اطلاعات خودی و به‌دست آوردن اطلاعات دیگران است. جنگجویان رسمی و غیررسمی این جنگ دیگر افراد نظامی نخواهند بود، بلکه جاسوس‌هایی هستند که حتی بدون خروج از منزل به اطلاعاتی حیاتی دسترسی پیدا خواهند کرد یا سیستم‌های حفاظتی شبکه‌های[2] خود را در برابر دیگران ایمن‌تر خواهند نمود. البته لازم است توجه کنیم که اخلاق جنگی در این جنگ‌ها با جنگ‌های گذشته تفاوت عمده‌ای خواهد داشت. این جنگ، رسمی نیست. کشورها در حین جنگ شبکه‌ای ادعا

---

1. Decentralize
2. Guard Networks Systems

خواهند نمود که با کشورهای دیگر در کمال صلح و تفاهم رابطه دارند و منکر هر نـوع جنـگ شبکه‌ای خواهند شد و درصورت افشاء (برای مثال، مورد افشاء شدن نفوذ هکرهای روسی بـه کامپیوترهای پنتاگون) ادعا خواهند کرد که ایـن اعمـال ازسـوی افـراد مـستقل از دولـت و بـا انگیزه‌های شخصی صورت گرفته است.

۶. ویژگی‌های نبرد اطلاعات استراتژیک

ویژگی‌های نبرد اطلاعات استراتژیک را در هفت محور کلی می‌تـوان مـورد بررسـی قـرار داد. دراین بخش ابتدا این هفت محور را ترسیم کرده، سپس به توصیف چالش‌ها و آسیب‌پذیری‌ها در هریک از این محورها و راه‌حل‌های موجود خواهیم پرداخت.[۱]

ویژگی‌ها	پیامدها
کم‌هزینه بودن تهدیدات را به‌شدت چندبرابر می‌کند	هرکس می‌تواند حمله کند
ازبین رفتن مرزهای سنتی، ایجاد مشکل می‌کند	شاید مشخص نشود چه کسی مورد حمله قرار گرفتـه، چه کسی حمله کرده، ... یا چه کسی مسئول آن است
مدیریت افکار و درک مردم، نقش‌ها را گسترش داده است	شاید نتوان تشخیص داد چه چیزی واقعیت دارد
اطلاعات استراتژیک هنوز در دسترس نیست	شاید ندانیم چه کسی دشمن ما خواهد بود... یا اهـداف و امکانات آنها چیست
هـشدارهای تـاکتیکی و بـرآورد حملـه، بـسیار دشوار است	شاید ندانیم که مورد حمله قرار گرفتـه‌ایـم، چـه کـسی حمله می‌کند... یا چگونه حمله می‌کند
ایجاد و حفظ ائتلاف‌ها دشوارتر خواهد بود	شاید به کسانی اتکا داشته باشیم که آسیب‌پذیرند
آسیب‌پذیری قلمرو (ایالات‌متحده) شـاید اهـرم فشاری در اختیار دشمنان قرار دهد	ایالات‌متحده احتمـالاً دیگـر بـه‌عنـوان قلمرویـی امـن نخواهد بود

---

۱. این متن اقتباسی است از:

Roger C. Molander; Andrew S. Riddile, Wilson, and Peter A., Wilson, **Strategic Information Warfare: A New Face of War,** Santa Marina, Calif: RAND, 1996, Chap. 4.

۶ـ۱. کم‌هزینه بودن

مهم‌ترین رخدادی که تقریباً همزمان با شکل‌گیری نبرد اطلاعاتی به‌وجود آمده، دسترسی کم‌هزینه به علوم حساس رایانه‌ای و بهره‌گیری از شبکه‌های پیچیده ارتباطی برای افزایش کارایی در مدیریت داده‌ها و اطلاعات بین تولیدکنندگان و مصرف‌کنندگان آن بوده است. این شرایط سبب افزایش قابل‌توجه تعداد، انواع و قابلیت‌های دشمنان بالقوه در جنگ‌های اطلاعاتی شده است. دیگر پیامد کم‌هزینه بودن، افزایش سریع پیچیدگی زیرساخت‌های اطلاعاتی و تأثیر این پیچیدگی بر دیگر ویژگی‌ها و جوانب است؛ مانند: ازبین رفتن مرزها، اطلاعات استراتژیک، هشدارهای تاکتیکی و برآورد حمله.

ضرورت‌های تجاری گسترده‌ای وجود دارد تا از این نکته اطمینان حاصل شود که شبکه‌ها و سیستم‌ها اطلاعاتی درحال پیدایش با کارایی بالایی فعالیت می‌کنند؛ به‌گونه‌ای‌که با کمترین نیاز به نگهداری حجم انبوه داده‌ها (به‌دلیل عدم اطمینان از نظام عرضه و تقاضا) بتوان اطلاعات مورد نیاز را مورد بهره‌برداری قرار داد. متأسفانه در بسیاری از موارد، جایگزینی کارایی با «حجم انبوه» سبب شکل‌گیری آسیب‌پذیری‌های جدید در مقابل حملات، به‌ویژه در مراحل آغازین تحول شبکه‌ها شده است. این پدیده که به‌سرعت درحال تغییر است، سبب پیدایش بازیگران توانا و شریری در عرصه فضای اطلاعاتی می‌شود که با سرعتی نزدیک به سرعت نور به گستره وسیعی از اهداف در زیرساخت‌های اطلاعاتی دسترسی خواهند داشت.

در چنین وضعیتی بسیاری از شبکه‌های پیشرفته و به‌هم‌پیوسته در معرض حمله طرف‌های مختلفی مانند: افراد متبحر، بازیگران غیرکشوری، سازمان‌های تبهکاری بین‌المللی و کشورهایی که دارای نیروهای آموزش‌دیده در زمینه جنگ‌های اطلاعاتی هستند، خواهند بود. اجزای اصلی این حملات شامل: دسترسی به شبکه‌های اطلاعاتی و مهارت درباره فایل‌های داده‌ها، سیستم‌های مدیریت داده‌ها یا سیستم‌های کنترل، آن‌هم در محیطی که بانک‌های اطلاعاتی، سیستم‌های کنترل و مدیریت به‌صورت فزاینده‌ای به یکدیگر متصل و به‌هم پیوسته هستند، می‌شود.

مهم‌ترین نمونه این پدیده، رشد انفجاری اینترنت است که در آن ده‌ها میلیون کاربر با بهره‌گیری از شبکه ارتباطی جهانی به ده‌ها هزار بانک اطلاعاتی - که در مقابل ورود غیرمجاز، بسیار کم یا هیچ محافظت می‌شود - دسترسی خواهند داشت. پیدایش اینترنت را می‌توان به آزاد شدن سریع زمین‌ها برای چرای چارپایان در اواخر قرن نوزدهم تشبیه کرد. این استعارهٔ غرب وحشی، مناسب و به‌جاست؛ زیرا امروزه این بحث مطرح شده است که آیا برای حفاظت از بانک‌های اطلاعاتی ازطریق رمزگذاری یا دیگر تکنیک‌ها درواقع باید نوعی سیم خاردار اطراف آنها کشید یا خیر؟

رمزگذاری در نقاط ورودی به بانک‌های اطلاعاتی مختلف، ورود غیرمجاز حمله‌کنندگان آماتور و با تکنولوژی پایین را دشوار می‌کند. درواقع بسیاری از کارشناسان اعتقاد دارند راه‌حل مقابله با آسیب‌پذیری زیرساخت‌های جهانی اطلاعات در آینده، با اتخاذ رویکردی آزادانه در برابر نفوذ کاربران شخصی، تجاری، غیرکشوری[1] و کشوری به تکنولوژی کدگذاری، ممکن خواهد بود. اینکه آیا چنین راه‌حلی در برابر ارزانی و کم‌هزینه بودن نبرد اطلاعاتی سبب بروز مشکلات برای نیروهای انتظامی و امنیت ملی کشور خواهد شد، کاری جداگانه می‌طلبد. البته باید توجه داشت که حداقل پیامد نفوذ کاربران به تکنولوژی کدگذاری، دشوار شدن فزاینده وظایف سازمان‌هایی است که در امر گردآوری اطلاعات، نظارت و شناسایی منابع حملات کامپیوتری فعالیت می‌کنند. با گسترش کدگذاری، طراحی سیستمی کارآمد برای هشدارهای تاکتیکی و برآورد حمله دشوارتر خواهد شد و اعلام هشدارهای استراتژیک نیز سخت خواهد بود.

برای مقابله با تهدیدات ناشی از این ویژگی اگر رویکردی اتخاذ کنیم که براساس آن به افراد و مؤسسات اجازه داده شود به کمک نرم‌افزارهای کدگذار، از دسترسی راحت کاربران به شبکه‌ها و سیستم‌های کنترل جلوگیری کنند، می‌توان انجام حملات جنگ‌های اطلاعاتی را دشوار ساخت. شایان ذکر است که استفاده گسترده از نرم‌افزارهای کدگذاری ممکن است با

---

1. Nonstate

رخی تهدیدها مقابله کند؛ ولی نمی‌تواند مانع حملات مستقیم فیزیکی یا بروز حمله از داخل سیستم و به‌وسیله یکی از اپراتورهای خائن شود.

علاوه‌بر اذعان به عملی بودن بروز تهدیدهایی که با هزینه اندک خواهد بود، به‌نظر می‌رسد ین ویژگی جدید نبرد اطلاعاتی مستلزم نوع جدیدی از «برآورد خطر» باشد.

۶ـ۲. کم‌رنگ شدن مرزهای سنتی

یکی از مهم‌ترین ویژگی‌های شکل‌گیری زیرساخت‌های اطلاعاتی جهانی (و به تبع آن زیرساخت‌های اطلاعاتی ملی)، کم‌رنگ شدن و محو تدریجی مرزهای جغرافیایی، اداری، قضایی و حتی مفاهیمی است که از لحاظ سنتی جزو موضوعات امنیت ملی بوده‌اند؛ برای مثال، مرزهای مشخص‌کننده حدود کشوری مستقل، به‌صورت فزاینده‌ای درحال ازبین رفتن هستند. همانند کشورها، عدم کنترل بر بازارهای مالی جهانی و ارتباط متقابل و روزافزون زیرساخت‌های اطلاعاتی آمریکا با شبکه‌های اطلاعاتی جهانی نیز به‌ناگزیر حاکمیت ملی را تضعیف خواهد کرد.

مهم‌ترین بعد چشمگیر محو تدریجی مرزها این است که دیگر نمی‌توان به‌وضوح بین منابع داخلی یا خارجی تهدیدات نبرد اطلاعاتی تمایز قائل شد. محو تدریجی مرزها سبب فزایش تنش بین سازمان‌های مرتبط با امنیت ملی و سازمان‌های انتظامی خواهد شد.

یکی دیگر از جوانب قضیه این است که تفاوت بین اقدام‌های ضدکشوری که شامل طیف وسیعی از فعالیت‌ها (از جرم و جنایت تا درگیری نظامی) است، از بین می‌رود. بدون وجود تمایز روشن و واضح جغرافیایی بین منابع داخلی و خارجی اقدامات ضد ملی، شناسایی قداماتی نظیر: جاسوسی، جرم و جنایت و اقدامات خصمانه بسیار دشوار خواهد بود. به‌دلیل وجود احتمال حمله به زیرساخت‌های اطلاعاتی از طریق شبکه‌های کامپیوتری، این احتمال به‌صورت گسترده‌ای وجود خواهد داشت تا کشورهایی که از لحاظ قدرت و ابزارهای نظامی و اقتصادی از رقبای خود ضعیف‌تر هستند، با به‌کارگیری اشخاص یا سازمان‌های بین‌المللی

فعال دراین‌زمینه اقدام به انجام عملیات نمایند که شناسایی منشأ آن (منبع صدور فرامین و دستورات) بسیار دشوار خواهد بود. دیگر نمونه‌های ازبین رفتن وجوه تمایز سنتی را می‌توان نامشخص شدن تفاوت میان عمومی و خصوصی، نظامی و تجاری، استراتژیک و تاکتیکی دانست. آخرین نکته‌ای که می‌توان در این‌باره گفت مربوط به «تأثیر سلاح‌ها»ست؛ بدین‌صورت که بین تأثیر موردنظر و تأثیر واقعی سلاح‌ها به‌ویژه درباره خسارات جانبی بر زیرساخت‌ها، اطمنیان‌خاطر وجود ندارد.

پیامد محو تدریجی مرزها این است که اگر کشوری مورد حمله قرار گیرد، نمی‌تواند دریابد که به چه چیزی حمله شده است؛ درنتیجه به سرعت نمی‌توان مشخص کرد که چه سازمان یا بخشی از جامعه باید مسئولیت واکنش به آن را برعهده گیرد.

۶ـ۳. مدیریت ادراک

با گسترش شبکه‌های کامپیوتری، هزینه ورود به این عرصه کاهش یافته، مرزهای حاکمیت ملی به‌تدریج محو می‌شود و بدین‌ترتیب بازیگران کشوری و غیرکشوری امکان خواهند یافت اطلاعات را که عنصر اساسی ادراک و تلقی مردم است، دست‌کاری کرده، تغییر دهند.

بحث را می‌توان با اینترنت آغاز کرد که به همراه رقیبان آن در ابتدای قرن جدید، شبکه‌ای را برای «تبلیغ» گستره وسیعی از بازیگران فراهم ساخته است. وقایع اخیر مکزیک در زمان شورش چیاپاس، نمونه روشنی را درباره استفاده از اینترنت برای جلب توجه رسانه‌های جمعی و نیز جلب حمایت سیاسی در مکزیک و سایر مناطق آمریکای شمالی و برای اهداف سیاسی و اقتصادی سازمان‌های ضد رژیم ارائه می‌دهد. با توجه به قضیه بمب‌گذاری در اوکلاهماسیتی، شواهد رو به تزایدی وجود دارد که سازمان‌های شبه‌نظامی متعددی از اینترنت برای جلب حمایت سیاسی و ارائه اطلاعات درست و گمراه‌کننده به سازمان‌های محلی استفاده کرده‌اند. گروه‌های فعال سیاسی و سازمان‌های غیردولتی خواهند توانست از اینترنت برای جلب حمایت سیاسی استفاده کنند.

درضمن این احتمال نیز وجود دارد که «حقایق» یک واقعه به‌صورت گسترده‌ای ازطریق متن، صدا، تصویر (مثلاً با استفاده از تکنیک‌های پیشرفته تصویری برای تحریف تصاویر) تغییر پیدا کنند. این تکنیک‌ها به بسیاری از بازیگران این امکان را می‌دهند تا ادراک و فهم مردم را مدیریت کنند یا با به‌راه انداختن تلاش‌های مربوط به دیپلماسی عمومی، حمایت داخلی از اقدامات دولت آمریکا را کاهش دهند. این تلاش‌ها نه‌تنها برای دولت آمریکا ایجاد مشکل می‌کنند، بلکه رسانه‌ها نیز به‌عنوان نهادی برای مخابره دقیق وقایع، با دشواری مواجه می‌شوند.

پیامد مستقیم این ویژگی آن است که تصمیم‌گیرندگان آمریکایی یا مردم این کشور ممکن است نتوانند دریابند که چه چیزی واقعی است.

۶ـ۴. اطلاعات استراتژیک

به‌دلیل دو ویژگی اصلی نبرد اطلاعاتی (کم‌هزینه بودن و ازبین رفتن تدریجی مرزها) دستگاه اطلاعاتی کشورها ممکن است در ارائه به‌موقع و صحیح اطلاعات استراتژیک درباره تهدیدهای کنونی و آینده نبرد اطلاعاتی به مقامات قوه مجریه با دشواری‌های عمده‌ای مواجه شوند.

شناسایی اهدافی که باید درباره آنها اطلاعات جمع‌آوری شود، بسیار دشوارتر خواهد بود. رویکرد ژئواستراتژیک که به‌صورت سنتی مورد استفاده قرار می‌گرفت و کشورها را به‌عنوان تهدید تلقی می‌کرد، امروزه در شرف کهنگی و محجور شدن است. امروز اهدافی که باید درباره آنها اطلاعات جمع‌آوری شود شامل: سازمان‌های غیردولتی، سازمان‌های تبهکاری بین‌المللی و بازیگران غیرکشوری می‌شود. اهمیت و بزرگی یک تهدید به توانایی‌های حمله‌کنندگان اطلاعاتی، اهداف و نیات آنها و نیز میزان آسیب‌پذیری اهداف بستگی دارد. توانایی‌های مهاجم ممکن است به‌دلیل ماهیت دینامیک فضای اطلاعاتی و ارتباطات راه دور، نرم‌افزارها، سخت‌افزارهای ریزپردازنده و تکنیک‌های دفاعی‌اش برای کدگذاری، کاهش پیدا کند. زیرساخت‌های اطلاعاتی در ابتدای قرن جدید شامل: طیف وسیعی از عناصر و امکانات در جامعه‌ای پیشرفته ازلحاظ اقتصادی و تکنولوژیک می‌شود. عناصر و امکانات زیرساخت‌ها عبارتند از:

۱. شبکه عمومی کنترل (سوئیچ)؛
۲. خطوط انتقال نفت و گاز؛
۳. شبکه‌های انتقال برق؛
۴. سیستم‌های کنترل حمل‌ونقل؛
۵. سیستم نقل‌وانتقال منابع مالی فدرال؛
۶. سیستم‌های مختلف نقل‌وانتقال وجوه بانک‌ها؛
۷. سیستم بهداشت و درمان.

درعین‌حال که آسیب‌پذیری‌های برخی از عناصر زیرساخت اطلاعات به‌خوبی شناسایی شده، بسیاری دیگر از آسیب‌پذیری‌ها هنوز ناشناخته باقی مانده‌اند.

تهیه و تدوین فهرست پایداری از تهدیدها، برای دستگاه اطلاعات بسیار دشوار خواهد بود. محیط جهانی برخلاف ساختار دوقطبی که ایستا بود، امروزه چندقطبی و پویا شده است.

۶ـ۵. هشدارهای تاکتیکی و برآورد حمله

به‌دلیل مشکل شدن جمع‌آوری اطلاعات استراتژیک و محدودیت‌های زمانی در بحران‌ها، پیامد ناتوانی در اعلام «هشدارهای تاکتیکی و برآورد حمله» بسیار دشوارتر و خطرناک‌تر خواهد شد. به‌نظر می‌رسد در آینده، برآوردها و پیش‌بینی‌های متعارضی درباره احتمال حمله یا رخدادها، ازسوی نیروهای انتظامی و دستگاه‌های اطلاعاتی به مقامات مسئول کشوری ارائه شود.

حمله‌ای که با استفاده از جنگ‌افزارهای اطلاعاتی انجام می‌شود می‌تواند عملیات استراتژیکی را با سرعتی بی‌سابقه انجام دهد و سپس عقب‌نشینی کند. یافتن به‌موقع عاملان حمله، اگر نگوییم غیرممکن، بسیار دشوار خواهد بود؛ به‌ویژه در بحران‌های شدیدی که در آنها وقت اندکی برای اجرای تحقیقات متعارف پلیسی وجود دارد.

با توجه به افزایش پیچیدگی شبکه‌های ارتباطی، سیستم‌های مدیریت بانک‌های اطلاعاتی و سیستم‌های کنترل، برخی از وقایع ممکن است نتیجه طراحی نامناسب یا بدشانسی باشد.

علاوه‌برآن ممکن است اقدامات تهاجمی استراتژیکی انجام شوند که براساس فعالیت چندساله برای کسب آمادگی، سیستم‌ها را مورد نفوذ قرار دهند. بسیاری از این اقدامات ممکن است به‌درستی مورد شناسایی قرار نگیرند.

۶ـ۶. ایجاد و حفظ ائتلاف‌ها

قدرت‌های بزرگ در آینده با این وضعیت مواجهند که ایجاد و استمرار ائتلاف با کشورهای خارجی جهت پشتیبانی از اقدام قهرآمیز برضد مخاصمات بین‌المللی، بسیار دشوار خواهد بود. این وضعیت احتمالاً با توجه به موضوعات چنداطلاعاتی نیز تشدید خواهد شد. قدرت‌ها در مقابل حملات نبرد اطلاعاتی به زیرساخت‌های اصلی خود، بسیار آسیب‌پذیر هستند. چند عامل این مشکل را افزایش می‌دهد: مشکل رعب‌آور تلاش برای حفظ قابلیت ارائه اطلاعات استراتژیک صحیح و هشدارهای تاکتیکی؛ زمانی‌که نبرد اطلاعاتی شدید درگیرد، حفظ ائتلاف بسیار دشوار خواهد شد. همچنین اگر یکی از شرکای ائتلافی به‌دلیل آسیب‌پذیری در مقابل نبرد اطلاعاتی به «حلقه‌ای ضعیف در زنجیره» تبدیل شود، مشکلات شدیدی در اجرای طرح و برنامه ائتلاف پیش خواهد آمد.

دیگر اینکه ممکن است بسیاری از کشورها در بخش‌های اصلی خود، آسیب‌پذیری‌های شدیدی داشته باشند (مثلاً ارتباطات، انرژی، حمل‌ونقل و امور مالی) و دشمن ممکن است برای تضعیف ائتلاف به آنها حمله کند. این آسیب‌پذیری‌ها در مراحل نخستین بهره‌گیری این کشورها از تکنولوژی اطلاعاتی، شدیدترند؛ زیرا در این مرحله به‌جای آنکه توجه این کشورها به امنیت سیستم‌ها باشد، بیشتر متوجه کسب توانایی‌ها و امکانات است. سیستم‌هایی که از خارج کشور (با عنوان مقرون به صرفه بودن ازلحاظ تجاری و سرعت دستیابی) تهیه می‌شوند، ممکن است آسیب‌پذیر باشند. این امر به‌ویژه درباره گسترش سریع تلفن همراه در کشورهایی که فاقد زیرساخت‌های تلفن‌های معمولی (سیمی) هستند، صدق می‌کند. نسل کنونی تلفن‌های همراه در مقابل شنود، ایجاد مزاحمت و سرقت کدهای رمز مشترکان، بسیار آسیب‌پذیرند. نسل

آینده تلفن‌های همراه کمتر آسیب‌پذیر خواهند بود؛ ولی هزینه‌های تغییر نسل ممکن است در کشورهایی با درآمد کمتر، آن را از انجام تغییرات سریع باز دارد.

۷. منابع در نبرد اطلاعاتی

نبرد اطلاعاتی، درباره عملیاتی است که منابع اطلاعاتی را هدف قرار می‌دهد یا از آنها استفاده می‌نماید. این منابع را می‌توان از نظر کاربردی به پنج گروه زیر طبقه‌بندی کرد: مخازن[1]، انتقال‌دهنده‌ها[2]، دریافتگرها (حسگرها)[3]، ثبت‌کننده‌ها[4] و پردازنده‌ها[5]. این طبقه‌ها به‌طور کامل جدا از یکدیگر نیستند؛ یعنی منبعی مفروض می‌تواند در آن واحد چند کاربرد داشته باشد. مردم و رایانه‌ها نمونه‌هایی از منابع دارای چند عمل به‌شمار می‌روند.

مخازن، رسانه‌های اطلاعاتی هستند که اطلاعات (و اطلاعات غلط) را در خود دارند. ازآنجاکه هر شیئی مقداری اطلاعات (مثلاً اطلاعاتی که ساختار آن را معین می‌کند) در خود دارد، پس تمام اشیا، مخازن اطلاعاتی هستند؛ ولی آنچه به‌طور ویژه مورد توجه است، اشیایی هستند که می‌توان به آنها محتوای اضافی داد. حافظه انسان، حافظهٔ رایانه، رسانه‌های چاپی، نوارها، دیسکت‌ها و ظرف‌های مخصوص آنها ازجمله این اشیا هستند. مخازن می‌توانند در داخل یکدیگر قرار گیرند؛ برای مثال، سندی را می‌توان در پوشه قرار داد، پوشه را در کابینت گذاشت، خود کابینت در اتاقی است که آن اتاق در ساختمانی قرار گرفته است. در رسانه‌های رایانه‌ای، داده‌ها در فایل‌ها گذاشته می‌شوند و فایل‌ها به‌نوبهٔ‌خود در فهرست‌های راهنما[6] ذخیره می‌شوند. در جهان مادی، لازمهٔ دسترسی یافتن به اطلاعات، گذر کردن از لایهٔ دفاعی هرکدام از آنهاست؛ ولی در جهان الکترونیک می‌توان لایه‌هایی را که در نرم‌افزار قرار داده شده دور زد؛ مثلاً اطلاعات دیسکت را می‌توان بدون باز کردن فایل یا بانک اطلاعاتی مربوطه یا گذشتن

1. Containers
2. Transporters
3. Sensors
4. Recorders
5. Processors
6. Directories

از سیستم فهرست راهنما به‌طور مستقیم خواند.

انتقال‌دهنده‌ها، سیستم‌های اطلاعاتی و اشیایی هستند که اطلاعات را از محلی به محل دیگر انتقال می‌دهند. انسان‌ها ـ که هنگام رفتن از جایی به جای دیگر با ارتباط رودررو با دیگران اطلاعاتی را همراه دارند یا حمل می‌کنند ـ خودروها و سیستم‌های فیزیکی حمل‌ونقل شامل: سیستم‌های تلفن و تلگراف، رادیو و تلویزیون، شبکه‌های رایانه‌ای نظیر: اینترنت و شبکه‌های سازمان‌ها در زمره انتقال‌دهنده‌ها محسوب می‌شوند.

دریافتگرها ابزارهایی هستند که اطلاعات را از اشیاء دیگر و به‌طور کلی از محیط استخراج می‌کنند و شامل: دریافتگرهای انسانی، دوربین‌ها، میکروفن‌ها، پویشگرها (اسکنرها) و رادارها می‌شوند.

ثبت‌کننده‌ها دستگاه‌هایی هستند که اطلاعات را در ظرف‌ها می‌گذارند. فرایندهای انسانی، چاپگرها، ضبط‌صوت‌ها و ضبط‌تصویرها ـ که صدا یا تصویر را روی نوار ضبط می‌کنند ـ و پرکننده‌های دیسکت‌ها ازجمله ثبت‌کننده‌ها به‌شمار می‌روند.

بالاخره، پردازشگرهای اطلاعات اشیایی هستند که اطلاعات را دست‌کاری[1] می‌کنند. مردم، ریزپردازنده‌ها، نرم‌افزارها و سخت‌افزارهای رایانه‌ها، پردازشگرهای اطلاعات هستند.

این منابع دست‌به‌دست هم می‌دهند تا اطلاعات بتواند از ظرفی به ظرف دیگر و در انواع سیستم‌های ترابری جریان یابد. دریافتگرها اطلاعات را از محیط فیزیکی برداشت می‌کنند. سپس این اطلاعات، کامپیوتری می‌شود، مورد پردازش قرار می‌گیرد، چاپ می‌شود، از رادیو و تلویزیون پخش می‌شود، در سیستم‌های مخابراتی و اینترنت انتقال می‌یابد و به دستگاه‌هایی که فرایندهای محیط مانند گرمایش و سرمایش را کنترل می‌کنند تغذیه می‌شود. این ارتباط متقابل موجب می‌شود که عملیات نبرد اطلاعاتی بر منابعی غیر از منابع موردنظر نیز اثر بگذارند؛ برای مثال، افرادی که به‌طور غیرمجاز به رایانه وارد می‌شوند با دست‌کاری در رکوردهای ذخیره‌شده

1. Manipulate

در رایانه‌های شرکت تلفن، تلفن‌ها را تغییر مسیر داده‌اند. آنها با ایجاد اختلال در رایانه‌های شرکت تلفن، در خدمات مخابراتی فرودگاه‌ها ایجاد اختلال کرده‌اند.

عبارت «زیربنای اطلاعات» به منابع اطلاعاتی مانند سیستم‌های مخابراتی که از یک صنعت، مؤسسه، یا جمعیت پشتیبانی می‌کنند اطلاق می‌شود. زیربنای اطلاعات یک شرکت مالی، دفاعی[1]، ملی[2] و جهانی[3] نمونه‌هایی از زیربناهای اطلاعات هستند.

منظور از «فضای اطلاعات» مجموع منابع اطلاعاتی موجود در یک مؤسسه است. برای مؤسسات بازرگانی، فضای اطلاعات عبارت است از: کارکنان، مدارک چاپی، سیستم‌های رایانه‌ای و مخابراتی، به‌علاوه تمام اطلاعات ساختاری که در محیط فیزیکی شرکت و سازمان داخلی رمزگذاری شده‌اند. «فضای سایبر»[4] نیز فضای اطلاعاتی است که از جمع کل شبکه‌های رایانه‌ای تشکیل شده باشد.

یک فضای اطلاعات که در زمان جنگ مورد توجه ویژه قرار می‌گیرد، فضای نبردی است که از تمام عناصر موجود در محیط فیزیکی ازجمله سیگنال‌های مخابراتی موجود در هوا تشکیل می‌شود. هرکدام از طرفین نبرد تلاش می‌کنند در عین محروم کردن هرچه بیشتر طرف دیگر از دسترسی به این اطلاعات، خود از آن اطلاعات حداکثر آگاهی را پیدا کنند. هرکدام از طرفین ممکن است در قلمرو طرف مقابل، اطلاعات غلط قرار دهد و در منابع اطلاعاتی مورد استفادهٔ دشمن خرابکاری کند.

۷ـ۱. ارزش منابع

منابع اطلاعات، برای مردم دارای ارزش هستند. این ارزش از دو جزء تشکیل شده است: ارزش مبادله و ارزش عملیاتی. ارزش مبادله توسط بازار تعیین می‌شود و قابل تبدیل به کمیت

---

1. Defence Information Infrastructure (DII)
2. National Information Infrastructure (NII)
3. Global Information Infrastructure (GII)
4. Cyberspace

است. این ارزش، قیمتی است که کسی حاضر است در مقابل آن منبع بپردازد.

ارزش عملیاتی تابع فوایدی است که می‌توان ازطریق استفاده از آن منبع به‌دست آورد. این ارزش نیز ممکن است قابل تبدیل به کمیت باشد، ولی همواره چنین نیست؛ مثلاً ممکن است رایانه‌ای به‌عنوان وسیله یادگیری، ایجاد امکانات، به‌دست آوردن شغل رضایت‌بخش‌تر یا کسب پول بیشتر مورد استفاده قرار گیرد. همچنین این رایانه می‌تواند برای ادارهٔ مؤسسه‌ای کوچک، نوشتن کتاب یا کارهای پشتیبانی که درآمدزا هستند و برای آینده ایجاد فرصت می‌کنند به‌کار رود. اطلاعات مربوط به تعیین محل نیروهای دشمن یا معالجه سرطان می‌تواند جان‌هایی را نجات دهد. یک کشف پژوهشی یا علمی جدید می‌تواند مورد بهره‌برداری قرار گیرد، درعین‌حال برای دیگران فرصت‌هایی ایجاد و به اقتصاد محلی یا جهانی کمک نماید. اطلاعات درباره برنامه سلاح‌های شیمیایی یا میکروبی یک کشور خارجی ممکن است به خنثی کردن آن برنامه و بازداشتن از استفاده از آنها در آینده منجر شود. در اکثر این موارد، قائل شدن ارزش دلاری برای منافع حاصله از این منابع مشکل است. خوشبختانه کمی کردن دقیق این ارزش، برای درک مفاهیم نبرد اطلاعاتی و اثر کلی عملیات تهاجمی و تدافعی، ضروری نیست. برای برآورد کردن اینکه عملیاتی خاص، اعم از تهاجم یا تدافعی ارزش اجرا دارد یا نه، برآوردی غیردقیق برحسب دلار یا عوامل دیگر، کافی است.

ارزش یک منبع برای یک طرف لزوماً با ارزش آن برای طرف دیگر مساوی نیست. برای یک بازیگر، ارزش منبع تابع شش عامل زیر است: نگرانی‌ها و تعهدات بازیگر، توانمندی‌های بازیگر، موجود بودن منبع برای آن بازیگر، موجود بودن منبع برای بازیگران دیگر، تمامیت منبع و زمان.

اولین و مهم‌ترین عامل، نگرانی‌ها و تعهدات بازیگر است. برای اینکه منبعی دارای ارزش باشد، باید به اقدامات و روندهایی که برای بازیگر اهمیت دارد کمک کند.

عامل دومی که به ارزش عملیاتی مربوط می‌شود توانمندی‌های بازیگر است. این توانمندی‌ها شامل: دانش، مهارت‌ها و ابزارهای مورد استفاده بازیگر می‌شود، ولی دسترسی به

منبع را دربرنمی‌گیرد؛ مثلاً یک فلاپی دیسک برای کسی که رایانه دارد ارزشمندتر است تا برای کسی که رایانه ندارد.

عامل سوم، در دسترس بودن منبع برای بازیگر است. اینکه منبع تا چه حد در دسترس بازیگر است تا از آن به‌طور مناسب استفاده کند موضوع این عامل است. در دسترس بودن، به مخفی بودن و محرمانه بودن اطلاعاتی که از بازیگر مخفی نگاه داشته می‌شود؛ مربوط می‌شود اما مفهوم وسیع‌تری هم وجود دارد: اینکه منبع را تا چه حد می‌توان دست‌کاری و محتوای اطلاعاتی آن را مشخص نمود، یا اینکه آیا منبع را می‌توان مشاهده کرد، پردازش نمود، تغییر داد، نسخه‌برداری نمود، توزیع کرد، یا به فروش رساند بخشی از این مفهوم وسیع است.

ارزش یک منبع با در دسترس بودن آن برای بازیگر نسبت مستقیم دارد. عامل چهارمی که در ارزش منبع تأثیر دارد، در دسترس بودن منبع برای بازیگران دیگر است. در نبرد اطلاعات، ارزش عملیاتی معمولاً با در دسترس بودن منبع برای بازیگران دیگر نسبت معکوس دارد. ارزش این نوع اطلاعات، تا حدی ناشی از انحصاری بودن آنهاست؛ یعنی اینکه آن اطلاعات از دسترس مخالفان و دشمنان به دور باشد. ارزش، از کمبود نیز ناشی می‌شود. اینکه بازیگر، تنها کسی باشد (یا یکی از معدود بازیگرانی باشد) که به اطلاعات دسترسی دارد، بسیار ارزشمندتر از دسترسی به اطلاعاتی است که به‌طور وسیع در اختیار همگان باشد. بااین‌حال پاره‌ای از اطلاعات وقتی توزیع می‌شوند، ارزش بیشتری پیدا می‌کنند.

عامل پنجمی که به ارزش منبع می‌افزاید، تمامیت آن است. منظور از تمامیت، کامل بودن، خوب بودن یا درجه درستی، کمال، اصلی بودن و قابل اعتماد بودن منبع است. تمامیت اطلاعات اغلب با موثق، قابل اطمینان، اصل و غیرقابل انکار بودن (یعنی کسی نتواند اطلاعات ارسال‌شده یا پردازش‌شده را منکر شود) همراه است و با آنها تفسیر می‌شود. ارزش منبع برای بازیگر ممکن است با تمامیت آن منبع نسبت مستقیم داشته باشد؛ اما همواره چنین نیست. فریب می‌تواند نقش بازی کند و بازیگر ممکن است از خراب کردن عمدی یک واسط اطلاعاتی، مثلاً با جعل داستان و منتشر کردن آن در اینترنت، سود ببرد.

عامل ششم و نهایی، زمان است. ارزش منبع در طی زمان، با توجه به نقش آن در عملیات، افزایش یا کاهش می‌یابد.

ازسوی‌دیگر می‌توان بین ارزش عملی و ارزش بالقوه یک منبع تفاوت قائل شد. ارزش عملی، ارزشی است که منبع، قبل از عملیات نبرد اطلاعاتی دارد؛ ولی ارزش بالقوه ممکن است بعد از عملیات وجود داشته باشد. اگر حمله‌کننده، دستاورد بالقوه ارزشمندی در عملیات نبیند (صرف‌نظر از اینکه دستاورد مورد انتظار، تحقق پیدا کند یا نه)، نبرد اطلاعاتی تهاجمی احتمالاً انجام نمی‌شود.

۷ــ۲. بازیگران

در هر عملیات جنگی اطلاعاتی، دو بازیگر اصلی وجود دارند که عبارتند از: بازیگر تهاجمی که عملیات علیه منبع اطلاعاتی خاصی را شروع می‌کند و بازیگر تدافعی که هدفش دفاع کردن در برابر آن حمله است.

۷ــ۳. تهاجم

اگرچه بازیگر تهاجمی اغلب «آدم بد» نشان داده می‌شود، همیشه چنین نیست.

بازیگران هر دو طرف می‌توانند افرادی باشند که به‌تنهایی عمل می‌کنند، با گروه‌هایی که دارای ساختار یا فاقد ساختار هستند، دوست باشند یا نباشند و در نهایت، ممکن است مورد حمایت قرار گیرند یا نگیرند.

بازیگر برای اینکه وارد نبرد اطلاعاتی شود باید دارای انگیزه، وسیله و فرصت باشد. انگیزه، تابع نگرانی‌ها و تعهدات اوست و وسیله‌ها توسط توانمندی‌ها و قابلیت دسترسی تعیین می‌شوند. فرصت نیز تابعی از دسترسی است؛ اما عوامل دیگری را نیز مانند: پیش‌بینی موفقیت عملیات، با مانع روبه‌رو نشدن یا گیر نیفتادن دربرمی‌گیرد. اگر در آغاز، دسترسی به میزان کافی نیست، باید قبل از تحقق اهداف (مثلاً خرابکاری در یک منبع اطلاعات) به دسترسی کافی رسید.

اگرچه تمامی اشخاص یا سازمان‌ها می‌توانند درگیر نبرد اطلاعاتی تهاجمی شوند، بیشتر عملیاتی که در عمل انجام می‌گیرد به چند طبقه کلی نسبت داده می‌شود، شامل: داخلی‌ها (خودی‌ها)، وارد شوندگان غیرمجاز به رایانه‌ها، جنایتکاران، شرکت‌ها، دولت‌ها و تروریست‌ها.

داخلی‌ها (خودی‌ها) عبارتند از: کارکنان سابق و موقت، پیمانکاران و اشخاص دیگری که از داخل به منابع اطلاعاتی یک سازمان دسترسی دارند. این گروه معمولاً بزرگ‌ترین تهدید سازمان محسوب می‌شوند. اینان به‌عنوان شکنندگان اطلاعات عمل می‌کنند و اطلاعات حساس متعلق به سازمان خود را به دولت‌های خارجی، رقبا و مجرمان سازمان‌یافته می‌فروشند. اقدام آنها طرح‌های تجاری و نظامی، عملیات اطلاعاتی و مسائل خصوصی افراد را دربرمی‌گیرد. داخلی‌ها در سیستم‌های رایانه‌ای کارفرمای خود خرابکاری می‌کنند و همراه با رمزهای تجاری از مؤسسه بیرون می‌روند تا شرکت‌های رقیب ایجاد کنند. حتی در مواقعی که آنها منبع اصلی یک حمله نیستند، خواسته یا ناخواسته، به بدکاران دیگر کمک می‌کنند. انگیزه آنها، پول، ایدئولوژی، انتقام و کمک به افراد خارج از مؤسسه است.

گروه بعدی افرادی هستند که به‌طور غیرمجاز وارد سیستم‌های رایانه‌ای می‌شوند. این افراد به زبان انگلیسی «هکر»[1] نامیده می‌شوند. این عنوان به هر فرد مسلط بر رایانه قابل اطلاق است؛ ولی در بحث از نبرد اطلاعاتی، معمولاً به کسی گفته می‌شود که سیستم‌های الکترونیکی به‌ویژه سیستم‌های رایانه‌ای و مخابراتی را شکسته یا وارد آنها می‌شود. ازجمله انگیزه‌هایی که آنان را به این عمل وامی‌دارد، هیجان، چالش و قدرت است. اگرچه بسیاری از این متجاوزان قصد دریافت پاداش مادی یا آسیب رساندن به سیستم‌های مورد تهاجم را ندارند، عده‌ای از آنها برای پول یا خراب کردن رایانه‌ها به این عمل مبادرت می‌کنند. به‌هرحال حتی وقتی نیت بدخواهانه وجود ندارد، این ورود غیرمجاز، به تمامیت منبع آسیب می‌رساند و برای صاحبان سیستم، چیزی بیش از شیطنت است.

---

1. Hacker

گروه سوم، یعنی جنایتکاران، منابع اطلاعات مالی مانند: حساب‌های بانکی یا شماره کارت‌های اعتباری یا مالکیت‌های معنوی را که قابل تبدیل به پول ازطریق فروش زیرزمینی است هدف قرار می‌دهند. آنها اغلب به‌صورت گروه‌های سازمان‌یافته عمل می‌کنند و انگیزه اصلی‌شان پول است. دلالان اطلاعات و آنانی که ویدئو، لوح فشرده (سی‌دی) و نرم‌افزارهای دزدی می‌فروشند جزء این گروه هستند.

شرکت‌ها و مؤسسات، گروه چهارم بازیگران هستند. اینان در زمانی‌که فعالانه درصدد کسب اطلاعاتی از رقبای خود هستند یا اسرار تجاری رقبای خود را به وسایل غیرقانونی مانند رشوه دادن به داخلی‌ها می‌ربایند، درگیر نبرد اطلاعاتی می‌شوند. آنها با انگیزه پول و موقعیت رقابتی، اطلاعات مربوط به مشتریان خود را می‌فروشند که این عمل تجاوز به حریم خصوصی آن مشتریان محسوب می‌گردد.

گروه پنجم، ادارات دولتی هستند. چندین ادارهٔ دولتی در نبرد اطلاعاتی تهاجمی دست دارند. ادارات اجرای قانون، سوابق و ساختارهای سازمانی مجرمان را هدف قرار می‌دهند تا شواهد و اطلاعات مربوطه را جمع‌آوری کنند. اداره اطلاعات در تلاش است تا به اسرار نظامی، دیپلماتیک و اقتصادی دولت‌ها، شرکت‌ها و رقبای خارجی دست یابد. آنها برای کسب اطلاعات به «موش کور»های داخلی و بازبینی‌های الکترونیکی بسیار متکی هستند. در زمان جنگ، واحدهای نظامی سیستم‌های اطلاعاتی کنترل و فرماندهی دشمن را منهدم می‌کنند. مقررات دولتی، به‌دلیل امنیت ملی و اهداف ایمنی عمومی، سخنرانی‌ها را کنترل می‌کنند و دسترسی به فناوری اطلاعات را محدود می‌نمایند.

گروه ششم، تروریست‌ها هستند. با توجه به آسیب‌های بالقوه‌ای که می‌توانند به زیرساخت‌های حساس مانند: خدمات اورژانس و سیستم‌های مالی وارد شوند، تروریست‌ها موردتوجه ویژه قرار دارند. آنها اطلاعات مربوط به اهداف خود را جمع‌آوری می‌کنند، به پخش تبلیغات مبادرت می‌ورزند و در ساختمان‌ها و تجهیزات فیزیکی خرابکاری می‌کنند.

این فهرست، شامل تمام بازیگران نیست، هرکس ممکن است به عملیات نبرد اطلاعاتی

تهاجمی مبادرت کند (مثلاً با دزدیدن اطلاعات، دروغ‌پراکنی و سد کردن راه دسترسی مشروع به اطلاعات). سایر گروه‌های بازیگران تهاجمی عبارتند از: فعالان سیاسی، افراطیون، تماشاگران و اراذل. این گروه‌ها به‌طور کامل از یکدیگر جدا نیستند؛ برای مثال، واردشونده غیرمجاز به سیستم الکترونیک می‌تواند درعین‌حال فعال سیاسی، تروریست داخلی و جاسوس شرکت نیز باشد.

در زمان مفروض، ممکن است چند بازیگر منبع واحدی را هدف خود قرار دهند؛ مثلاً ممکن است صدها نفر درصدد دسترسی به رایانه‌های شرکت معینی باشند یا چند دولت برای جمع‌آوری اطلاعات مربوط به هدفی تلاش کنند. در نبرد اطلاعاتی تدافعی، تمام این تهدیدهای چندگانه باید درنظر گرفته شوند.

۷ـ۴. دفاع

نبرد اطلاعاتی تدافعی توسط همه کس (فرد، سازمان یا دولت) انجام می‌گیرد. در سطح افراد، دفاع در خدمت حفظ حریم خصوصی، منافع فردی، وضعیت رقابتی و به‌طور کلی بهروزی فرد مدافع است. در سطح سازمان، دفاع به‌منظور حفظ وضعیت رقابتی و منابع سازمانی انجام می‌گیرد. در مورد دولت‌ها، هدف از دفاع عبارت است از: حفظ امنیت ملی، امنیت اقتصادی، ایمنی همگانی و نظم و قانون. نقش دولت‌ها در نبرد اطلاعاتی تدافعی و حفظ اطلاعات در چند مقوله می‌گنجد؛ شامل: تحقیق درباره جرم و تعقیب مجرمان، ضد اطلاعات، دفاع ملی، برقراری محافظت‌های قانونی، تعیین استانداردها و پژوهش و توسعه فناوری‌های دفاعی جدید.[1]

۷ـ۵. نقش دوگانه

طرف‌هایی که درگیر نبرد اطلاعاتی هستند ممکن است هم نقش دفاعی و هم نقش تهاجمی

1. The Joint Chief of Staff, **Information Assurance: Legal, Regulatory, Policy and Organization Considerations**, Sep. 17, 1997.

داشته باشند. در پاره‌ای از وضعیت‌ها، دو طرف ممکن است برای دست یافتن به برتری در پاره‌ای از منابع با هم مبارزه کنند و در این مبارزه از عملیات تهاجمی و تدافعی استفاده نمایند. آنچه برتری اطلاعاتی را تعیین می‌کند این است که کدام بازیگر می‌تواند از منبع، بیشتر استفاده کند که این امر بیشتر بستگی به میزان دسترسی هریک از بازیگران به منبع دارد. البته توانمندی‌های آنان نیز عامل مؤثری است؛ ممکن است بازیگری دسترسی کمتری داشته باشد، ولی به‌علت دارا بودن دانش، مهارت یا ابزارهای برتر، از منبع بیشتر استفاده نماید.

فصل سوم

استراتژی و تاکتیک‌های نبرد اطلاعات

- درآمد
- محیط منازعه
- چگونگی تفکر درباره نبرد اطلاعات
- اهداف الکترونیکی
- اهداف سطح بالاتر

۱. درآمد[1]

طی دهه اخیر، فناوی اطلاعات توسط سیاست‌گذاران، فعالان سیاسی، بوروکرات‌های بین‌المللی، رهبران بازرگانی و روشنفکران به‌عنوان کاتالیزوری برای تغییر و تحول اجتماعی، ایجاد رشد و توسعهٔ اقتصادی، صلح و جهان‌وطنی بین‌المللی، آزادی شخصی و قدرت‌یابی فردی مورد حمایت قرار گرفته است. به‌نظر می‌رسد انقلاب فناوری اطلاعات نیز همانند انقلاب صنعتی پیش از آن، درحال ایجاد طبقه جدید حاکم، اقتصاد جدید و جامعه‌ای نو باشد. جای تعجب نیست که متفکران استراتژیک و متخصصان امنیتی شیفته چگونگی دگرگونی عملیات و جنگاوری نظامی توسط فناوری اطلاعات شده‌اند. رهبران نظامی و روشنفکران معتقدند که فناوری اطلاعات می‌تواند الگوی جنگاوری به صرفه‌تر و منعطف‌تر عصر اطلاعات را که با استفاده از نیروهای ماهرتر و فناوری‌های «هوشمند»، ریسک کمتری را ازنظر تلفات دربردارد، جایگزین الگوی جنگ تخریبی کلاسوتزی عصر صنعتی نماید. درست همان‌طورکه عصر هسته‌ای، منطق بازدارندگی را بر تخریب برتری داد، در عصر اطلاعات نیز منطق اختلال، توان رقابت با منطق تخریب را داراست؛ به این دلایل، عصر اطلاعات در جنگاوری نشان‌دهندهٔ نقطه عطفی دراین‌زمینه است.

فناوری اطلاعات همواره در جنگاوری، مهم و در ارتقای میزان کارایی نظامی حیاتی بوده

---

۱. این متن اقتباسی است از:

Matt Bishop and Emily O. Goldman, "The Strategy and Tactics of Information Warfare", **Contemporary Security Policy, Vol. 24, No.1, Apr. 2003.**

است. تأسیس شبکهٔ تلگراف، به‌طرز قابل توجهی، عملکرد و عملیات نظامی و میزان کارایی نیروهای نظامی را طی جنگ داخلی آمریکا و جنگ‌های اتحاد آلمان ارتقا بخشید.[۱] اختراع بی‌سیم در آغاز قرن بیستم، نشانگر بُعد مهمی از انقلاب نیروهای دریایی بود که بسیاری آن را با تحول کشتی‌های جنگی قدرتمند ـ که نیروی خود را از موتورهای توربین می‌گرفتند ـ و تحول طیف گستردهٔ زیردریایی‌ها و اژدرها مرتبط می‌دانستند. بی‌سیم همچنین ابزاری برای هشداردهی استراتژیک بسیار پیشرفته به‌شمار می‌رفت. طی دوران بین دو جنگ، رشد سریع کاربرد رادیو و بعدها پیدایش رادار، تأثیر عظیمی بر عملیات نظامی داشت. به‌کارگیری حملهٔ برق‌آسا از سوی ارتش آلمان درست به اندازه مکانیزه‌سازی و هوانوردی به توانایی رادیو برای هماهنگ کردن نیروهای عظیم، سریع و به‌شدت پراکنده، بستگی داشت.[۲] شبکهٔ همبسته دفاع هوایی انگلستان نیز به مجموع زیرساخت‌های رادیویی و راداری بسیار وابسته بود.[۳] استمرار بین این مثال‌های تاریخی و زمان حال، در تلاش‌های نیروی نظامی آمریکا برای به‌کارگیری سیستم‌های اطلاعات درحال ظهوری مانند GPS (سیستم‌های موقعیت‌یاب ماهواره‌ای)، جهت آگاه شدن از مانورهای زمینی و هدف‌گیری دقیق، مشهود است.

اطلاعات به‌عنوان «محتوا»، متمایز از اطلاعات به‌عنوان «مجرا»، همواره یکی از ابعاد مهم استراتژی در نبردها و درگیری‌ها بوده است، چه در زمانی که وجود داشته و چه در زمان غیاب آن.[۴] بدبینی کارل فون کلاوسویتس دربارهٔ قابل اطمینان بودن اطلاعات و مأموران اطلاعاتی در

---

1. Geoffrey L. Herrera, "Inventing the Railroad and Rifle Revolution: Information, Military Innovation and the Rise of Germany", paper prepared for the center for Strategic and Budgetary Assessments workshop on **Military Revolutions: The Role of Information Capabilities,** Washington DC, 4-5 March, 2002.
2. Robert Citino, "Beyond Fire and Movement: Command, Control, and Information in the German Blitzkrieg". Ibid.
3. David Zimmerman, "Information and the Air Defense Revolution, 1917-1940". Ibid.

۴. اطلاعات به‌عنوان «محتوا» اشاره به علامتی دارد که حاوی محتوای معناداری است و قابلیت انتقال، چه در شکل اطلاعات سری یا به صورت پیغام‌هایی بین فرماندهان و نیروها دارد. اطلاعات به‌عنوان «مسیر» بیشتر بر جریان، یا بر ارتباطات علامت‌ها تمرکز دارد تا محتوای آنها. دیدگاه اطلاعات به‌عنوان مسیر، تجزیه و تحلیل را بر فناوری‌های اطلاعاتی متمرکز می‌سازد که اجازهٔ انتقال و دریافت پیغام را می‌دهد.

سطوح تاکتیکی و عملیاتی وی را به این امر سوق داد تا در کتاب «دربارهٔ جنگ»[1] بر ضرورت به‌حداکثر رساندن و تمرکز بر نیروهای خود، حفظ نیروهای ذخیره و اطمینان از قدرت درونی و تجربهٔ رهبران تأکید ورزد. ازطرف‌دیگر سان تزو[2] در کتاب «هنر جنگ»[3]، فریبکاری، اطلاع‌رسانی غلط و آگاهی از درونی‌ترین افکار و نقشه‌های دشمن را کلیدهای غافلگیر کردن او و شاید حتی پیروزی بدون خونریزی دانسته است.

چیزی که عصر اطلاعات را بی‌همتا می‌سازد، این واقعیت است که اطلاعات «به‌عنوان» جنگاوری به اندازهٔ اطلاعات «در» جنگاوری مهم شده است.

اطلاعات مانند گذشته تنها ابزار ارتقای میزان کارایی فناوری‌های مرگبار نیست، بلکه امکان حملات غیرمرگبار را که می‌تواند دشمن را ناتوان ساخته، شکست داده، تحت فشار گذاشته یا آن را بازدارد، فراهم کند. عصر اطلاعات با گسترش ابزار و تکنیک‌های حملهٔ اطلاعاتی، حوزه‌های نبرد اطلاعات و تأمین‌کنندگان آن را بسط داده است. جنگ امروزه در میدان نبرد، در بازار[4] و علیه زیرساخت‌های جامعهٔ مدرن رخ می‌دهد و حمله‌کنندگان علاوه‌بر نظامی‌گران حرفه‌ای شامل افراد و گروه‌های خصوصی می‌شود که جنگاوری را از انحصار دولت خارج کرده است.

بااین‌حال حتی باوجود تغییر مجموعهٔ ابزارها، حوزه‌ها و جنگاوران، منطق جنگاوری همان‌طور باقی مانده است. جنگاوری، ترتیب و هماهنگی حملاتی است برای دستیابی به اهداف سطح پایین‌تر تکنیکی یا «الکترونیکی» که بخشی از سلسلهٔ عملیات گسترده‌تر برای کسب اهداف سطح بالای سیاسی، مادی یا نمادین محسوب می‌شوند. فهم این مطلب که چگونه انواع مختلف اهداف تکنیکی می‌توانند در دستیابی به اهداف استراتژیک سطح بالاتر کمک کنند، مستلزم پیوند دادن قلمروی استراتژیست‌ها و دانشمندان رایانه است. تنها آن زمان است که تکنیک‌های حملهٔ اطلاعاتی را می‌توان به‌طرز مؤثری در خدمت استراتژی به‌کار برد و

1. On War
2. Sun Tzu
3. Art of War
4. Marketplace

مفاهیم استراتژیکی چون: بازدارندگی، تشدید، مقابله‌به‌مثل و ارتباط را در استقبال از امکانات جدید ارائه‌شده توسط نبرد اطلاعات وفق داد.

این فصل، استراتژی و تاکتیک‌های نبرد اطلاعات را ازطریق نشان دادن چگونگی ارائه راه‌های جدید دستیابی به اهداف سیاسی، مادی و نمادین سنتی توسط ابزار جنگ الکترونیکی ارزیابی می‌کند. همچنین چگونگی تغییر محیط کنونی منازعه، ماهیت آسیب‌پذیری‌ها و تهدیدات را توسط قابلیت‌های اطلاعات مورد بحث قرار می‌دهد و مروری بر چگونگی تفکر دربارهٔ نبرد اطلاعات و بحث دربارهٔ منطق زیربنایی و پیش‌نیازهای تکنیکی انواع مختلف حملات اطلاعات خواهد داشت و با بررسی برخی از مهم‌ترین تدارکات و گسست‌های بین گذشته و حال و با توجه به استراتژی و تاکتیک‌های نبرد اطلاعات، نتیجه‌گیری خواهد نمود.

۲. محیط منازعه

با انفجار اخیر فناوری‌های اطلاعات، وابستگی فزایندهٔ جوامع پیشرفته به آنها و رشد سریع قابلیت‌های کاربرد اطلاعات و مختل کردن جریان آن، نبرد اطلاعات، نقشی اساسی در تقریباً تمامی مباحث مربوط به روابط خصمانه، چه نظامی و چه تجاری پیدا کرده است. عقل متعارف حاکی از این امر است که ما وارد عصری شده‌ایم که اطلاعات، تنها مؤلفه‌ای ثانویه در عملیات متعارف نظامی و بازرگانی نیست، بلکه تبدیل به عرصهٔ اصلی منازعه و مقابله شده است.

نبرد اطلاعات به‌طرزجدی ادامه‌دهندهٔ روندهایی است که پیش از این در مسیر تحول جنگ بوده‌اند. تلاش برای بازداشتن یا شکست دشمن ازطریق دور زدن تخریب نیروها و حملهٔ مستقیم به اجتماع آن، همانند بمباران استراتژیک و هدف‌گیری هسته‌ای ضدارزشی[1]، به زمان قبل از عصر فناوری اطلاعات برمی‌گردد. تکنیک‌های نبرد اطلاعات به‌آسانی آرایش گسترده‌تری از ابزار و شیوه‌ها و توانایی هدف‌گیری دقیق‌تری را ازطریق ابزار غیرکشنده بر

1. Counter-Value Nuclear Targeting

خطوط حیاتی که جوامع پیشرفته بر آنها تکیه دارد در اختیار حمله‌کنندگان قرار می‌دهند؛ نظیر: شبکه‌های نیرو، سیستم‌های تلفن، شبکه‌های حمل‌ونقل و سیستم‌های هدایت هواپیماها. فناوری اطلاعات همچنین می‌تواند نبرد متعارف را دقیق‌تر کرده، بدین‌طریق کارایی حملات انفجاری شدید را ارتقا بخشد. در اینجا نیز، فناوری اطلاعات روندهایی را در جنگاوری ادامه می‌دهد که میزان کشندگی نیروهای نظامی را طی زمان افزایش بخشیده است.

به‌عبارت‌دیگر فناوری اطلاعات، محیط منازعه و چگونگی تفکر ما را دربارهٔ آسیب‌پذیری دستخوش تغییر کرده است. کنترل اطلاعات و دانش، موتور مرکزی پیش‌برندهٔ عمل انسان است که در رشد باورنکردنی قدرت رایانه‌ای، افزایش وابستگی به فناوری اطلاعات در معاملات بازرگانی (کارت‌های اعتباری، بانکداری الکترونیکی)، بالا رفتن برق مصرفی و بیشتر از همه، وابستگی فزاینده بر اینترنت مشهود است. توزیع ویروس رایانه‌ای که طبق فرمان فعال می‌شود، دزدی الکترونیکی سرمایه از یک شرکت کارت اعتباری، انتشار اطلاعات غلط ازطریق اینترنت یا رسانه‌ها، یا دست‌کاری در پست‌های الکترونیکی، همگی نکته‌های جدیدی از آسیب‌پذیری را به جامعهٔ معاصر عرضه می‌کنند.

در مقابل، فناوری اطلاعات، پیشرفته‌ترین و قدرتمندترین جوامع ازنظر شاخص‌های سنتی را به آسیب‌پذیرترین جوامع در برابر چنین حملاتی تبدیل کرده است. مشخصهٔ بارز عصر اطلاعات «شبکه» است که از در دسترس و مهیا بودن اطلاعات و سرعت محاسبه‌ای و ارتباطی، برای سازماندهی و اشاعهٔ ارزان و مؤثر دانش بهره می‌برد.[1] قدرت شبکه در درجهٔ ارتباط‌دهی آن نهفته است: ارتباط‌دهی می‌تواند باعث افزایش رفاه و میزان کارایی نظامی باشد، اما آسیب‌پذیری‌هایی را نیز ایجاد می‌کند. سازمان‌های نظامی به‌شدت اطلاعاتی، نسبت به نبرد اطلاعات آسیب‌پذیرترند، صرفاً بدین‌دلیل که به اطلاعات وابسته‌ترند؛ درحالی‌که ضرورتی ندارد نیروی متخاصم وابسته به اطلاعات باشد تا بتواند خطوط اطلاعاتی تکنولوژیک و حیاتی

1. See Richard J. Harknett, "Integrated Security: A Strategic Response to Anonymity and the Problem of the Few", **Contemporary Security Policy,** Vol. 24, No. 1, Apr. 2003.

دشمن را مختل کند. جوامع وابسته به اطلاعات نیز بیشتر نسبت به نفوذ شبکه‌های رایانه‌ای، بانک‌های اطلاعاتی و رسانه‌ها در حملات صورت‌گرفته بر خطوط اصلی ارتباطی نظیر: ارتباطات، معامله‌های مالی، حمل‌ونقل و شبکه‌های منابع انرژی که کارکرد جوامع مدرن به آنها وابسته است، آسیب‌پذیرترند. از دیدگاهی متقابل، احمقانه است که گروهی با وضعیت مالی خوب و دارای انگیزه، زیرساخت فنی دشمن را مورد حمله قرار ندهند.

فناوری اطلاعات همچنین نحوهٔ تفکر ما را دربارهٔ تهدیدها تغییر داده است. انقلاب اطلاعات بازیگران ضعیف‌تر ازنظر سنتی را ازطریق اشاعه و توزیع مجدد قدرت توانمند ساخته است. نبرد اطلاعات تنها منحصر به تعاملات بین‌دولتی نیست. افراد و بازیگران غیردولتی، چه شرکت‌ها و چه گروه‌های ذی‌نفع، سازمان‌های جنایتکار، یا گروه‌های تروریستی می‌توانند تا حدودی به شیوه‌های نبرد اطلاعات دست یابند. اداره حسابداری دولتی[1] ایالات متحده تخمین می‌زند که ۱۲۰ گروه یا کشور، درحال توسعهٔ قابلیت‌های تهاجمی نبرد اطلاعات بوده یا دارای آن هستند. ضرورتی ندارد کشوری جامعهٔ اطلاعاتی با فناوری بالا داشته باشد تا بتواند به قابلیت‌های نبرد اطلاعات دست یابد؛ زیرا این قابلیت‌ها، نسبتاً ارزان و در دسترس بوده، دارای ریشه‌های تجاری هستند. هزینه‌های ورود نسبتاً ارزان بدین معنی است که اشاعهٔ فناوری‌های اطلاعات، احتمالاً بسیار سریع‌تر از سلاح‌های هسته‌ای و هوافضایی به‌پیش خواهد رفت.

با این توصیف، اطلاعات به یکی از باارزش‌ترین کالاها و سرمایه‌های استراتژیک تبدیل شده است. توانایی یک کشور (یا شرکت) در تولید و استفاده از اطلاعات و حفاظت از سرمایه‌های اطلاعاتی خود، به‌معنای حفاظت از امنیت ملی (یا شرکتی) خود و تضمین رفاه شهروندان (یا سهامداران) خویش است. سیستم‌های اطلاعات، عرصهٔ اصلی عملیات و شیوهٔ بنیادینی برای اجرای عملیات تهاجمی بوده، نبرد اطلاعاتی عنصر اساسی هر «استراتژی» نزاع یا تقابل محسوب می‌شود.

1. U.S. Government Accountability Office (GAO)

۳. چگونگی تفکر دربارهٔ نبرد اطلاعات

به‌نظر می‌رسد تفکر در این مقوله در قالب طبقه‌بندی مفهومی صورت‌گرفته در جدول ۱ سودمند باشد. این چهار حوزهٔ حمله، بسیاری از رده‌بندی‌های رایج دربارهٔ نبرد اطلاعات را دربرمی‌گیرد. براین‌اساس شیوه‌ها یا ابزار حمله و اهداف مورد حمله را می‌توان به‌طور عمده در دو ردهٔ فیزیکی یا الکترونیکی طبقه‌بندی نمود.

شیوه‌ها (ابزار) حمله	هدف حمله	
	فیزیکی	الکترونیکی
فیزیکی (پرتاب جرم یا انرژی)	۱ ● جنگ سنتی؛ ● حملهٔ فیزیکی ارتقایافته توسط الکترونیک؛ ● بمباران امکان، تجهیزات و تسلیحات نظامی یا غیرنظامی؛ ● تروریسم.	۲ ● نبرد اطلاعات انفجاری؛ ● حملات فیزیکی به زیرساخت‌های اطلاعاتی (برای مثال حملهٔ ۱۱ سپتامبر کارکرد تلفن‌های همراه را تحت تأثیر قرار داد)؛ ● به‌کارگیری سلاح‌هایی با انرژی هدایت‌شده که سرویس‌های دیجیتالی را نابود یا مختل می‌کند.
الکترونیکی (پرتاب اطلاعات)	۳ ● حملهٔ فیزیکی با شیوه‌های الکترونیکی؛ ● حمله بر سیستم هواتوردی؛ ● اخلال سیستم کنترل ترافیک هوایی؛ ● حمله بر دستگاه‌های دیجیتال ویژه و تخصصی که قدرت الکتریکی را کنترل کرده، جلوی سدهای آب را می‌گیرند.	۴ ● نبرد اطلاعاتی غیرمرگبار؛ ● حملات برای ازکاراندازی سرویس‌ها؛ ● کرم‌ها و بمب‌های منطقی که در سیستم‌های اطلاعاتی تعبیه می‌شوند.

جدول ۱. حوزه‌های حمله

شوارتو[1] بین انواع نبرد اطلاعاتی شخصی، شرکتی و جهانی تمایز قائل شده است. بدین شکل که نبرد اطلاعاتی شخصی، افراد را هدف قرار داده، درحالی‌که اهداف نبرد اطلاعاتی شرکتی منافع بازرگانی، تجاری، اقتصادی، و نبرد اطلاعاتی جهانی، سرمایه‌های مربوط به منافع مالی را مورد هدف قرار می‌دهند.[2] راه معمول‌تر تمایز اهداف، جداسازی حوزه‌های نبرد اطلاعات «استراتژیک» و «میدان جنگ» است که اولی شامل اهدافی است در قلمرو اجتماعی و دومی، در قلمرو نظامی. نبرد اطلاعاتی به‌طور عمده اهداف نوین نظامی (مثل نیروهای دفاع هوایی دشمن و تسهیلات راداری) را برای نیروهای متعارف و الکترونیکی دربرمی‌گیرد.[3] همچنین در مورد اهداف غیرنظامی نوین برای نیروهای الکترونیکی، مانند حملات اخلالگر سرویس‌ها بر زیرساخت‌های مهم ملی یک کشور، بسیار به‌کار می‌رود.[4] باوجوداین تمایزات مذکور، این واقعیت را در پرده‌ای از ابهام می‌برد که آنچه واقعاً جدید است، توانایی رو به گسترشی است که با توجه به ماهیت متغیر قابلیت‌های بازیگران دولتی و غیردولتی و آسیب‌پذیری‌های فزایندهٔ جامعهٔ پیشرفته برای مختل کردن اطلاعات و شبکه‌هایی که کارهای مهم روزانهٔ سیستم‌های مدنی، تجاری و نظامی را حمایت می‌کنند، به‌وجود آمده است. تمایز غیرنظامی ـ نظامی نیز در جهانی که سیستم‌های نظامی به‌طور فزاینده‌ای از زیرساخت‌های اطلاعاتی غیرنظامی و مدنی استفاده کرده، به آنها وابسته‌اند و درجایی‌که وجوه اشتراک مهمی در آسیب‌پذیری‌های سیستم‌های اطلاعات نظامی و غیرنظامی وجود دارد، حتی کم‌اهمیت‌تر و

1. Shwartau
2. Winn Schwartau, **Information Warfare: Chaos on the Electronic Superhighway,** New York: Thunder's Mouth, 1994.
3. Roger W. Barnett, "Information Operations, Deterrence, and the Use of Force", **Naval War College Review,** Vol. 51, No. 2, Spring 1998, pp. 7-19; Timothy.L. Thomas, "Deterring Information Warfare: A New Strategic Challenge", **Parameters,** Winter 1996-97, pp. 81-91.
4. See Harknett in this volume; L. Sullivan, Jr., **Meeting the Challenges of Regional Security**, Carlisle, PA: US Army War College Strategic Studies Institute, 1994; G. F. Wheatley and R. E. Hayes, **Information Warfare and Deterrence**, Washington DC: National Defense University Press, 1996.

غیرسودمندتر می‌نماید.[۱]

علی‌رغم ویژگی این دوران به‌عنوان عصر اطلاعات، به‌طور قطع حملات همچنان قابلیت‌های فیزیکی و الکترونیکی را تلفیق خواهند کرد؛ مثل: کاربرد فناوری اطلاعات در عملیات تلفیقی تسلیحاتی، جهت بهبود کارایی حملات شدید انفجاری. شیوه‌های حمله در این مورد بیشتر به‌صورت فیزیکی باقی می‌مانند و اطلاعات تنها کارایی و دقت حملهٔ فیزیکی را بالا می‌برد. در آیندهٔ نزدیک، غیرممکن است که به‌ویژه ارتش‌های ملی استراتژی‌های صرفاً غیرفیزیکی جنگ را اتخاذ نمایند.[۲] تخریب فیزیکی همچنان نزدیک‌ترین هدف قابل توجه باقی خواهد ماند و حملات الکترونیکی احتمالاً در حمایت از عملیات مرگبار در صحنهٔ جنگ و علیه سرزمین کشور متخاصم به‌کار خواهد رفت. خانه شماره یک جدول ۱ این ویژگی‌های جنگاوری سنتی و حملهٔ فیزیکی ارتقایافته با ابزار الکترونیکی را بیان می‌کند. فناوری‌های اطلاعاتی، حملات متعارف را به‌عنوان توانمندسازهای فناوری‌های موجود ازطریق بالا بردن توانایی‌های یافتن اهداف، هدایت آتش به سمت آنها و نیز تسهیل برنامه‌ریزی و ارتباطات میان نیروهای خودی افزایش می‌دهد. در بسیاری از درگیری‌های نظامی پس از جنگ سرد، ازجمله: جنگ خلیج‌فارس، کوزوو و افغانستان، فناوری‌های اطلاعات به‌طور مؤثری برای حمایت و ارتقاء جنگاوری تخریبی سنتی در جنگ به‌کار رفته‌اند.

خانه شماره دو جدول، این ایده را مطرح می‌کند که سیستم‌های اطلاعاتی که عملیات جوامع مدرن امروزی و سازمان‌های نظامی را از پیش مهیا می‌کنند، می‌توانند به‌طور مستقیم مورد هدف حملات فیزیکی قرار گیرند. نبرد اطلاعاتی انفجاری، سیستم‌های اطلاعاتی را با

---

۱. برکوتیز گزارش می‌دهد که تقریباً ۹۵ درصد تمام ارتباطات نظامی ازطریق خطوط تجاری صورت می‌گرفت و اینکه ایالات متحده اکثر ریزپردازنده‌های مورد استفاده در سیستم‌های نظامی را فروشندگان تجاری تهیه می‌کرد. رجوع شود به:
Bruce D. Berkowitz, "Warfare in the Information Age", **Issues in Science and Technology**, Fall 1995, pp. 59-66.

2. See Chris C. Demchak, "Wars of Disruption: International Competition and Information Technology-Driven Military Organizations", **Contemporary Security Policy**, Vol. 24, No. 1, Apr. 2003.

نیروهای آتشین (جِرمی یا انرژی) مورد هدف قرار می‌دهند. حمله‌های فیزیکی با تسلیحات متعارف بر اهداف فرمان و کنترل و زیربناهای مهم شهری، نظیر: سیستم‌های تولید و انتقال نیروی برق، از مشخصه‌های عملیات نظامی اخیر غرب بوده است. این حملات می‌توانند عواقبی بسیار فراتر از تخریب مستقیم سرمایه‌های فیزیکی به‌عنوان پیامد ازدست دادن سرویس‌های خدماتی در سراسر جامعه داشته باشند. در سال‌های اخیر، توجه به سمت مقولهٔ جدیدی از نیروی آتشین (تسلیحات انرژی هدایت‌شده) چرخیده است که در مقایسه با تجهیزات ضربه‌زنندهٔ سنتی که دستگاه‌های ارتباطی را ازکار می‌اندازند اما ازنظر فیزیکی خراب نمی‌کنند، از ریزموج‌های با قدرت بالا برای ازکار انداختن اهداف الکترونیک استفاده می‌کنند. نسل جدید سلاح‌های انرژی هدایت‌شده «به‌منظور برتری جستن بر نوع تخریبی است که EMP[1] (فشار الکترومغناطیسی) هسته‌ای بر الکترونیک وارد می‌کند؛ اما با طیف بسیار کمتر، با کنترل بیشتر خسارات و بدون آن‌همه تخریب فیزیکی و رادیواکتیویتهٔ همراه با آن».[2]

تجزیه و تحلیل ما به‌طور جزئی بر حملات الکترونیکی متمرکز است که علیه اهداف فیزیکی و الکترونیکی نشانه می‌روند. خانه شماره سه، حملهٔ فیزیکی مبتنی‌بر الکترونیک، تخریب اهداف فیزیکی را به شیوه حمله بر سیستم‌های فنی زیربنایی دربردارد. این حملات ممکن است مرگبار بوده، جان‌ها و اموال را، اگرچه غیرمستقیم نابود سازد. توجهات اخیر به پتانسیل استفاده از اینترنت توسط تروریست‌ها برای هدف قرار دادن دستگاه‌های دیجیتال تخصصی جلب شده است؛ ازجمله: سیستم‌های کنترل توزیع‌شده (DCS) و سیستم‌های کنترل و داده‌های نظارتی (SCADA) که کلیدهای راه‌آهن را به‌راه انداخته، فلکه‌های موجود در لوله‌های آب، نفت و گاز را تغییر و تنظیم می‌کنند. این دستگاه‌های دیجیتال کنترلی به‌طور روزافزونی به اینترنت وصل می‌شوند و از امنیت اساسی برخوردار نیستند. به‌علاوه، خدمات

1. Electromagnetic Pulse (EMP)
2. Seth Schiesel, "Taking Aim at an Enemy's Chips", **New York Times**, 20 Feb. 2003, pp. El, E5.

شهری در سراسر جهان، به تکنسین‌ها امکان دست‌کاری از راه دور کنترل‌های دیجیتالی را می‌دهد و اطلاعات چگونگی این کار نیز به‌طور وسیعی در دسترس است.[۱]

نبرد اطلاعاتی برای درگیری‌هایی به‌کار برده می‌شود که تنها در حوزهٔ اطلاعات و سیستم‌های اطلاعات صورت می‌پذیرد. خانه شماره چهار این وجه خالص نبرد اطلاعاتی یا آنچه را ما جنگاوری غیرکشنده می‌نامیم دربردارد. این ابزار «دیجیتال» و اهداف شامل: عقاید جمعیت مردمی و رهبری طرف متخاصم و سیستم‌های اطلاعات اقتصادی و سیاسی است که کارکرد جامعه به آن بستگی دارد.

شاید بارزترین مشخصهٔ درگیری در عصر اطلاعات، ظرفیت تحت فشار قرار دادن و بازدارندگی طرف‌های متخاصم و تحت تأثیر قرار دادن و شکل دادن به محیط استراتژیک توسط راه‌های غیرمرگبار است. فناوری‌های اطلاعات که در روشی غیرتخریبی به‌کار می‌روند، می‌توانند در خدمت طیفی از اهداف درگیری بازدارنده قرار گیرند و چنانچه در حمایت از رژیم‌های کنترل صحت‌سنجی تسلیحاتی یا عملیات صلح به‌کار روند، موجب ارتقای شفافیت و ایجاد اعتماد و احتمالاً جلوگیری از وقوع درگیری می‌شوند. توانایی‌های بالای ردیاب‌ها برای کشف استقرارات نظامی و اشاعهٔ اطلاعات سری آنها می‌تواند موجب کاهش غافلگیری استراتژیک شده، از بروز درگیری جلوگیری نماید. از فناوری‌های اطلاعات نیز می‌توان در مقابله با تروریسم و جرایم بین‌المللی ازطریق ایجاد بانک داده‌های جهانی بهره برد که حرکت‌ها و فعالیت‌های این بازیگران فراملی را ردیابی می‌کنند. فناوری‌های اطلاعات احتمالاً می‌توانند از نسل‌کشی و برخوردهای قومی «پیش» از شروع آنها، با جایگزینی خطابه‌های ملی‌گرایانهٔ تحریک‌آمیز توسط اطلاعات دقیق جلوگیری نمایند.[۲]

اعتقاد بر آن است که فناوری اطلاعات همچنین به‌طور فزاینده‌ای از روشی غیرکشنده طی

---

1. Barton Gellman, "The Cyber-Terror Threat", **Washington Post National Weekly Edition,** 1-4 July 2002, pp. 6-7.

2. Joseph S. Nye, Jr. and William A. Owens, "America's Information Edge". **Foreign Affairs**, Vol. 75, No. 2, March-Apr. 1996, pp. 20-36.

جنگ و به‌عنوان جایگزین روش‌های شدید انفجاری ازطریق عملیات الکترونیکی به‌کار گرفته خواهد شد که ظرفیت هماهنگی طرف متخاصم را (چه نظامی چه اجتماعی) مورد هدف قرار می‌دهد نه سرمایه‌های فیزیکی را، و به‌جای تخریب مستقیم، آنها را مختل می‌نماید. اهداف نهایی رقابت و مقابله همان باقی می‌مانند: ممکن است سیاسی، مادی یا نمادین باشند یا توسط کشورها، سازمان‌ها یا بازیگران شخصی دنبال شوند؛ اما سلاح‌ها به‌جای فیزیکی، الکترونیکی بوده، به‌جای جرم یا انرژی، اطلاعات پرتاب می‌کنند و اهداف موردنظر، چه نظامی و چه غیرنظامی، سیستم‌های دیجیتالی یا ظرفیت‌های هماهنگی زیربنایی قابلیت‌های فیزیکی خواهند بود نه خود این قابلیت‌ها. در واقع نزدیک‌ترین[1] ابزار فنی حمله می‌تواند تخریب اطلاعات و سیستم‌های اطلاعاتی باشد؛ ولی اکثر مواقع با توجه به منابع محدود و آسیب‌پذیری سیستم‌ها، اختلال آن سیستم خواهد بود.

دلایل دوگانهٔ این امر عبارتند از: نخست، انقلاب فناوری اطلاعات، انتظارات از درگیری را تغییر داده است. در جوامع دموکراتیک امروزه، شاهد زوال مشروعیت کشتار و نیز بازتعریفی از بی‌گناهان هستیم که شامل اعضای غیرنظامی جامعهٔ طرف متخاصم نیز می‌شود[2] و مجموع این عوامل هرچیزی به‌غیر از کشتار بسیار دقیق را نیز در جوامع غربی به‌طور فزاینده‌ای غیرقابل قبول ساخته است. سرعت و دقت قابلیت‌های تحمل‌ناپذیر بودن میزان و شدت تلفات، عدم تمایز بین اهداف در حملات تخریبی و حمله بر بی‌گناهان ازسوی جوامع دموکراتیک، جذابیت این نوع نبرد اطلاعات را افزایش داده است.

دوم اینکه، به‌دلیل تسلط ایالات متحده بر صحنهٔ نبرد جهانی در زمینهٔ سلاح‌های متعارف، احتمال متوسل شدن دولت‌های خارجی و بازیگران غیردولتی بر استراتژی‌های نامتقارن مثل نبرد اطلاعات وجود دارد. حمله به سیستم‌های شبکه رایانه‌ای یکی از راه‌های ایجاد توازن در

---

1. Proximate
2. Chris C. Demchak, "Watersheds in Perception and Knowledge: Twenty Years of Military Technology", **Draft Manuscript**, June 1999.

برابر برتری ابردشمن متعارف است. برای بازیگران ضعیفی که نمی‌توانند قابلیت فیزیکی لازم برای صدمه زدن یا تحت تأثیر قرار دادن حریف‌های قدرتمند را مهیا کنند، حملات الکترونیکی به سرمایه‌های اطلاعاتی ممکن است استراتژی مطلوبی باشد. اگر طرف مقابل نیز جامعه و نیروی نظامی بسیار اطلاعاتی‌شده‌ای داشته باشد، مورد هدف قراردادن سیستم‌های اطلاعاتی آن منطقی به‌نظر می‌رسد؛ به‌ویژه سیستم‌هایی که حاوی اطلاعات سری دربارهٔ تاکتیک‌ها و استراتژی حریف بوده، فرمان، کنترل، هدایت قابلیت‌ها و سرمایه‌ها را به‌عهده دارند. این امر شامل زیربنای کارکرد جامعه و اقتصاد کشور متخاصم نیز می‌شود.

فهم این شکل از نبرد اطلاعات، چالش‌برانگیزتر از جنگ است؛ زیرا مرز بین صلح و جنگ را در پرده‌ای از ابهام فرو می‌برد. با توجه به توان تکنولوژیکی اختلال، انگیزهٔ مختل کردن به‌صورت پیشگیرانه به‌منظور «آماده‌سازی میدان جنگ» قبل از آغاز بحران یا خشونت‌های متعارف، یا برای ازکار انداختن سیستم جنگاوری طرف متخاصم ازطریق ایجاد نقصان کامل یا ناقص در آن، قوی است. یک عملیات سرکوبی اطلاعاتی پیش از جنگ ممکن است ارادهٔ دشمن را برای جنگیدن درهم بکوبد، اما آیا این ضربهٔ اول شامل استفاده از زور نیز هست؟[1] مرز صلح و جنگ ممکن است در عمل، بی‌معنی شود، به‌علاوه دیگر به خودی خود چیستی میدان نبرد در بافت نبرد اطلاعاتی واضح و روشن نیست؛ آیا وقتی کسی از بین نمی‌رود، واقعاً جنگی در میان است و آیا بازیگر درصورتی‌که تنها با ابزار الکترونیکی مورد حمله واقع شود انواع پرسنل و تجهیزات خود را هزینه خواهد کرد؟

هدف نهایی نبرد اطلاعات (کاربرد سرمایه‌های اطلاعاتی در خدمت استراتژی) پرهزینه‌تر کردن جنگ یا صحنهٔ رقابت برای حریف است. چنان‌که حریف به خواست خود تسلیم شده یا دیگر درگیر جنگ یا وارد تقابل بازار نشود، همواره نزدیک‌ترین مقصد بدین‌منظور، لطمه زدن به امنیت اطلاعاتی دشمن است. امنیت اطلاعاتی بر سه اصل استوار است: محرمانه بودن،

1. Thomas G. Mahnken, “War in the Information Age”, **Join: Force Quarterly,** Winter 1995-96. pp. 39-43.

تمامیت (بی‌نقصی) و در دسترس بودن (رجوع شود به جدول ۲)[1]. محرمانه بودن، نگهداری از اسرار است. تمامیت شامل: ارزیابی و حفظ قابل اعتماد بودن داده‌هاست. در دسترس بودن نیز امکان دسترسی به داده‌ها و سیستم‌ها را جهت استفاده دربرمی‌گیرد. هر حمله در نبرد اطلاعات، به یکی یا بیشتر از این موارد لطمه وارد می‌کند.

به‌طورکلی تمامی حملات در نبرد اطلاعاتی، ضربه‌ای هستند بر امنیت اطلاعاتی، خود اطلاعات یا سیستم‌هایی که اطلاعات را گردآوری، فرآوری و منتشر می‌کنند. اهداف آن نیز قابلیت‌های گردآوری، فرآوری و اشاعهٔ عقاید، دانش و اطلاعات دشمن است. در عرصهٔ نظامی، هدف حملات اطلاعاتی، فرستادن پیغام‌هایی است برای اقناع دشمن جهت توقف جنگ، اجتناب از آن و تخریب یا اختلال در کانال‌های ارتباطی آن به‌منظور تحت تأثیر قرار دادن پیشبرد استراتژی و توانایی جنگیدن یا مقاومت کردن دشمن. این پیغام‌ها ممکن است مستقیم (با هدف رهبران غیرنظامی و نظامی و نیروهای مسلح) یا غیرمستقیم (با هدف عموم مردم) باشند که حمایتشان برای جنگاوری، ضروری است. در عرصهٔ تجاری، هدف تحت تأثیر قرار دادن رفتار بازیگران در بازار (رقابت‌کنندگان، مشتریان، عرضه‌کنندگان و عموم) برای دستیابی به اهداف بازرگانی است.

امنیت اطلاعاتی	هدف حمله	هدف تکنیکی
محرمانه بودن	بهره‌کشی از سیستم‌های اطلاعاتی دشمن	دزدی یا استفادهٔ غیرقانونی از داده‌های ارزشمند
تمامیت	توزیع اطلاعات غلط یا بی‌اطلاعی	فاسد یا جرح‌وتعدیل ساختن اطلاعات یا سیستم‌های اطلاعاتی دشمن
در دسترس بودن	دریغ داشتن، نابود کردن، یا ازکار انداختن سیستم‌های اطلاعاتی دشمن	ازبین بردن اطلاعات کلیدی: فلج کردن سیستم‌های اطلاعاتی دشمن

جدول ۲. حمله به امنیت اطلاعاتی

1. Schwartau, Winn.opcit, p.265.

فراتر از این توضیح کلی، طیف گسترده‌ای از روش‌های حمله وجود دارد. اغلب گفت‌وگوها درباره نبرد اطلاعاتی بر دوگانگی بین تخریب و اختلال تمرکز دارد؛ اما تفاوت‌های فاحشی بین مختل و ناتوان کردن، ازکار انداختن، فاسد کردن و به‌تأخیر انداختن وجود دارد. تکنیک‌های کمتر از تخریب، دارای یورشگرهایی هستند با توانایی درجه‌بندی کردن حملات خود. به‌علاوه تخریب ممکن است فیزیکی یا منطقی باشد. در نهایت، پیشرفت‌های صورت‌گرفته در زمینهٔ فناوری اطلاعات به‌طرز شگرفی روش‌های اغفال دشمن، انحراف توجهات، تحریف، تنظیم و کنترل را گسترش داده‌اند.

اصل و اساس نبرد اطلاعاتی مبتنی بر خانه شماره چهار از جدول ۱ است؛ لذا ضروری است پیش‌نیازهای منطقی و تکنیکی زیربنایی انواع مختلف حملات اطلاعاتی را با تمرکز عمده بر این مورد، یعنی جنگاوری غیرمرگبار مورد بحث قرار داد. تفکر دربارهٔ اهداف تکنیکی یا الکترونیکی و اهداف سطح بالای سیاسی، مادی یا نمادین سودمند می‌نماید. ما ابتدا اهداف تکنیکی حمله، ازجمله استفاده از منابع الکترونیکی برای ازکار انداختن سیستم‌ها را مورد بحث قرار می‌دهیم. صحبت دربارهٔ این اهداف الکترونیکی به‌همان اندازه که در مورد نبرد اطلاعاتی استراتژیک (یا حملهٔ مستقیم به سرزمین اصلی) کاربرد دارد، بر نبرد اطلاعاتی در صحنهٔ نبرد نیز قابل انطباق است. باوجوداین اهداف الکترونیکی به‌طور مستقیم تأثیر عمده‌ای بر جامعه باقی نمی‌گذارند، بلکه شامل تأثیراتی هستند که بر سیستم‌ها و زیرساخت‌ها وارد می‌شوند. تمایز بین اهداف الکترونیکی و اهداف سطح بالاتر حائز اهمیت است. اهداف الکترونیکی اساسی‌ترند؛ زیرا بیشتر از آن خُرد نمی‌شوند. اهداف سطح بالاتر نتیجهٔ حمله‌ای برای دستیابی به اهداف الکترونیکی هستند؛ به‌نحوی‌که تأثیر دستیابی به آن اهداف، دستیابی به هدف عام‌تر سیاسی، مادی یا نمادین را نیز دربردارد. هر عملیاتی، به احتمال زیاد متشکل از چندین هدف مختلف الکترونیکی است (رجوع شود به جدول ۳).

در آنچه به‌دنبال می‌آید، هر هدفی را جداگانه مورد بحث قرار می‌دهیم. اگرچه، اهداف مختلف الکترونیکی و درنتیجه انواع مختلف حمله می‌توانند و احتمالاً باید تلفیق شده تا به

هدف نهایی حمله‌کننده دست یابند، کسب یک هدف مطلوب ممکن است مستلزم نتایج میان‌مرحله‌ای نیز باشد؛ برای مثال، فرض کنید یورشگری خواهان نظارت یا کنترل طرف مقابل بوده، برای انجام این امر، نیاز به گمراهی دشمن به‌منظور دست‌کاری سیستم جهت نظارت بر آن داشته باشد. بنابراین دو نوع حمله باید صورت گیرد: اولی، شامل فعالیت زیادی است که احتمالاً بدان پی برده می‌شود، اما نیازمند ایجاد یک‌سری دفاع است. این باعث انحراف توجه دشمن از دومین حمله است که شامل مجموعه حملات ظریف‌تری برای دست‌کاری سیستم جهت قرار دادن ضبط‌های حساس به تماس در مکان‌های مناسب و در نتیجه دستیابی به هدف موردنظر می‌شود.

۴. اهداف الکترونیکی

تخریب مستلزم ناتوان ساختن سیستم به‌نحوی است که قابل بازیافت نباشد و باید مجدداً ساخته یا ایجاد شود. تخریب ممکن است در عرصهٔ مجازی یا فیزیکی رخ دهد؛ اما نکته کلیدی اینجاست که عاملی در عرصهٔ مجازی است که ماشهٔ تخریب را می‌کشد.

کلاوسویتس طرفدار اصل تخریب به‌عنوان سودمندترین راه نیل به اهداف سیاسی و کوتاه‌ترین و امن‌ترین راه برای شکست دادن دشمن و تحمیل ارادهٔ خود است. تخریب معمولاً مستلزم حداکثر تمرکز نیروی فیزیکی بر نقطه‌ای مشخص، به‌منظور وارد آوردن صدمه‌ای جبران‌ناپذیر بر نیروهای مسلح، یا «مرکز ثقل» دشمن است. همچنین، قطعی‌ترین روش برای دستیابی به اهداف سیاسی است و درصورت موفقیت، پرخرج‌ترین و درصورت شکست، پرصدمه‌ترین راه محسوب می‌شود. اگرچه «اصل تخریب» کلاوسویتس، معمولاً معادل تخریب فیزیکی است، هندل[1] دراین‌خصوص می‌نویسد که «منظور کلاوسویتس از تخریب، لزوماً نابودسازی یا انهدام دشمن نیست، بلکه او به تخریب ارادهٔ دشمن برای جنگیدن نیز استناد می‌کند».[2] به‌عبارت‌دیگر تخریب، هر دو جنبه فیزیکی

1. Handel

فیزیکی و اخلاقی نیروهای دشمن را شامل می‌شود.

هدف حمله	آماج حمله	تاکتیک‌ها	نوع هدف
نابودی[1]	در دسترس بودن	وارد کردن اطلاعاتی که باعث تخریب سیستم می‌شود، کاهش سرعت بازیابی صفحات در مانیتورها	الکترونیکی
ناتوان‌سازی، ازکاراندازی و مختل کردن[2]	در دسترس بودن	مسیرهای اهداف؛ سرویس‌دهی، سیستم مختل‌شده (حملهٔ عدم سرویس‌دهی توزیع‌شده)؛ دادهٔ مرگبار (فرستادن بستهٔ مخصوصی که منجربه انجماد سیستم و ناتوان‌سازی مؤثر آن است)؛ برخی کرم‌ها و ویروس‌ها	الکترونیکی
به‌تأخیر انداختن[3]	در دسترس بودن تمامیت، (برای مثال، قابل اعتماد بودن تنزل اطلاعات بر اثر مرور زمان)	جلوگیری از دریافت پیغام‌های فوری (برای مثال، آنهایی که پرداخت را در قراردادها یا دریافت تجهیزات مهم را در صحنه‌های مختلف نظامی تأیید و قانونی می‌کنند)؛ افزایش ترافیک در برخی قسمت‌های شبکه برای افزایش زمان دریافت پیغام‌ها، افزایش باروری سرورها	الکترونیکی
انحراف توجه و گمراهی[4]	در دسترس بودن	انحراف توجه و منابع هدف؛ پنهان داشتن سایر حملات یا به‌تأخیر انداختن کشف آنها، به نمایش گذاشتن حملات بچه‌گانه درحالی‌که سایر حملات با ظرافت بیشتری در حال انجامند	الکترونیکی
تحریف[5]	محرمانه بودن تمامیت	محتوای اهداف در مقابل مسیرها و خطوط ارتباطی؛ مدیریت برداشت؛ عملیات روان‌شناختی	الکترونیکی
نظارت و کنترل[6]	محرمانه بودن تمامیت	رمزشکنی؛ دادن اطلاعات غلط (تقلید علامت شناخته‌شده چنان‌که گیرنده نتواند علامت ساختگی را از علامت واقعی تشخیص دهد)؛ مکان‌های تصویر آینه؛ استفاده از تکنیک‌های مختلف برای پوشاندن هویت طرف رسوخ‌کننده به شبکه یا سیستم	الکترونیکی

---

1. Destroy
2. Disable, Cripple, disrupt
3. Delay
4. Divert and distrac
5. Distort
6. Monitor and control

نوع هدف	تاکتیک‌ها	آماج حمله	هدف حمله
نمادین	نمایش توانایی‌ها با حمله به اهداف پرارزش، سیستم‌های به‌شدت محافظت‌شده، یا با انجام حمله‌های همزمان	محرمانه بودن تمامیت در دسترس بودن	خودنمایی کردن[1]
سیاسی	حمله بر زیرساخت‌های برقی، آبی و پزشکی برای به حداکثر رساندن درد و رنج اجتماعی	در دسترس بودن	مجازات کردن[2]
سیاسی	شبیه‌سازی و تمرین‌های تأثیرگذار، حملات اطلاعاتی پیش از جنگ علیه شبکه‌ها یا رهبری زمان و کنترل برای درهم کوبیدن ارادهٔ جنگیدن	در دسترس بودن	بازداشتن[3]
سیاسی	حملات محدود که قدرت صدمه و تحمیل درد درجه‌بندی شده و خسارت وادار کردن به اطاعت را به نمایش بگذارد	تمامیت در دسترس بودن	تحت فشار قرار دادن[4]
نمادین	نفوذ به سیستم رایانه‌ای بانک؛ تغییر فایل‌های مهم روی سیستم برای اجازهٔ ورود کاربران غیرقانونی جهت تغییر/ حذف فایل‌های کاربر به‌طور غیرمنتظرانه؛ تروجان‌های کامپیوتری	تمامیت	ازبین بردن مشروعیت و اطمینان[5]
مادی	جاسوسی صنعتی؛ پرده‌پوشی اطلاعات؛ ورود غیرقانونی به فایل‌ها و کپی کردن آنها؛ ایجاد ورودی‌های خصوصی برای ورود مجدد؛ نصب برنامه‌های ردیاب برای کسب اطلاعات و رفتار کاربر	محرمانه بودن تمامیت	دست‌کاری بازار[6]
مادی	نفوذ به سیستم رایانه‌ای بانک برای انتقال پول به درون یا بیرون از حساب‌ها؛ نفوذ به کامپیوتر رئیس اداره برای تغییر نمرات ترمیک، اخاذی؛ ایجاد مانع برای دستیابی به سرویس‌های حریف	محرمانه بودن تمامیت در دسترس بودن	نفع شخصی[7]

جدول ۳. اهداف و تاکتیک‌های حملات اطلاعاتی

1. Swagger
2. Punish
3. Deter
4. Coerce
5. Undermine confidence and legitimacy
6. Market manipulation
7. Personal gain

تخریب همواره نیازمند دانش چگونگی تعامل سیستم با موجودیت‌های خارجی است و این امر به‌همان اندازه که در دنیای فیزیکی صحت دارد، در دنیای مجازی نیز صادق است. تخریب فیزیکی به‌خصوص مستلزم دانش دربارهٔ محیط سیستم مانند: ویژگی‌های سخت‌افزاری یا مکان آن است، دو مثال درحال تغییر: سرعت بازیافت برخی رایانه‌های کهنه‌تر (که باعث سوختن آنها می‌شود) و نیز تعدیل برنامه‌ریزی سیستم‌های الکترونیکی هوابری است که هواپیما را کنترل می‌کند (و می‌تواند باعث سقوط هواپیما شود). سرعت بازیابی، یکی از کارکردهای سخت‌افزار مانیتور است. رایانهٔ الکترونیکی هوابری در موقعیتی پرمخاطره قرار گرفته، سلامت آن بستگی به صحت برنامه‌ریزی (و ورودی‌های) آن دارد. در هر دو مورد، حمله برای تحت‌الشعاع قراردادن هرگونه محدودیتی است که به‌منظور تضمین کارکردهای سیستم در محدوده‌های قابل قبول اعمال شده است.

تخریب منطقی ـ که در آن سخت‌افزار سیستم رها شده، اما منطق یا داده‌های سیستم غیرهوشمند و غیرقابل بازیافت می‌شوند ـ معمولاً مستلزم تخریب فیزیکی اطلاعات پشتیبانی ست. اگر هیچ اطلاعات پشتوانه‌ای موجود نباشد، حذف کردن نرم‌افزار یا داده‌ها برای موفقیت حمله کافی است و این امر نیازمند وارد کردن رمز برای حذف اطلاعات (برای مثال، با استفاده از حملهٔ ازدیاد بافرها)، تحریک رمز مستقر در سیستم (مانند آنچه در برخی سرورها وجود دارد)، یا به‌دست آوردن امتیازات (برای مثال، با ضربه زدن به یک سرور ممتاز) است. به‌منظور تعیین اینکه کدام‌یک از این رویکردها عملی و مناسب‌تر است، پورشگران سیستم را برای تشخیص اینکه کدام سرورها فعالند و نیز آیا هر یک از سرورهای فعال دارای این قابلیت‌ها هستند، مورد بررسی دقیق قرار می‌دهند. این بررسی‌ها ممکن است به تشخیص اطلاعات یا ویژگی‌های سرور نیاز داشته یا صرفاً فرمان‌های پیاپی را برای تشخیص عکس‌العمل آنها بفرستند.[1]

1. Fyodor, "The Art of Port Scanning", <http: //www.insecure.org/nmap/namp_doc.html>; Dustin. Lee, et al., "Detecting and Defending Against Web-Server Fingerprinting", **18th Annual Computer Security Applications Conference, 10-14 Dec. 2007.**

حمله‌کننده نیازمند اطلاعاتی دربارهٔ سیستم است، تا مؤثرترین راه تخریب آن را شناسایی کند. بنابراین حمله‌ای با هدف تخریب، با نوعی تجزیه و تحلیل رابطهٔ هدف با محیطش آغاز خواهد شد. این مرحله نیز ممکن است منطقی باشد، که دراین‌صورت حمله‌کننده هدف را بررسی می‌کند، یا فیزیکی باشد، که در این مورد حمله‌کننده، دستورالعمل و توضیحاتی دربارهٔ سیستم موردنظر و کاربردهای آن به دست خواهد آورد. دراین‌صورت، بررسی هدف، ویژگی‌هایی را به‌دنبال دارد که به یورشگر امکان کشف اطلاعات موردنظر برای آغاز حمله را می‌دهد؛ اما این اطلاعات ازطریق دستورالعمل‌ها به‌دست می‌آید. بنابراین سطح بررسی ممکن است بسیار پایین‌تر باشد.

پیشگامان حمله که قصد نابودی سیستم مورد هدف را دارند، نیازمند شناسایی راه‌هایی هستند که ازطریق آنها سیستم با محیط خود تعامل دارد. این حالت در مقابل، مستلزم شناسایی نوع سیستم موردنظر و کارکرد آن است. بررسی سرورهای شبکه‌ای به ایجاد این اطلاعات کمک خواهد کرد. به‌علاوه حملات، کارکردها و مؤلفه‌های خاصی از هدف را مورد حمله قرار می‌دهند.

ناتوان ساختن، تجهیزات را غیرعملی، اما قابل ترمیم باقی می‌گذارد؛ برای مثال، ازطریق راه‌اندازی مجدد. با ازکار انداختن، تجهیزات به عملکرد خود ادامه داده، اما برخی کارکردهای اصلی (آنهایی که برای هدف یا منظور سیستم اساسی‌اند) از کار می‌افتند؛ برای مثال، یک سرور پست الکترونیکی ممکن است دیگر قادر به فرآوری پست الکترونیکی نبوده، اما به سایر درخواست‌ها پاسخ دهد. با مختل کردن، تجهیزات به کارکرد خود ادامه داده، اما دارای نقصان‌های ادواری یا تغییر غیرمنتظرهٔ پیغام‌ها با حرکت از نقطه‌ای به نقطهٔ دیگر خواهند بود. یکی از تاکتیک‌های اصلی دستیابی به این نتایج، عدم سرویس‌دهی است که البته مقوله جدیدی در جنگاوری نیست. با توجه به اینکه بمباران کردن هدف، آن را از کار می‌اندازد، حملات الکترونیکی امکان ناتوان‌سازی، ازکاراندازی، اختلال غیرمرگبار و نیز اختلال پیشگیرانه به‌منظور آماده‌سازی صحنهٔ نبرد قبل از آغاز خشونت‌های متعارف را به انسان می‌دهد. در عرصهٔ نظامی، هدف حملهٔ عدم سرویس‌دهی، کور و کر کردن دشمن و جلوگیری از دسترسی آن به

اطلاعاتی است که برای جنگ و فرمان نیروها ضروری است. اگرچه اپراتورهای نرم‌افزارهای رایانه‌ای که رایانه‌های دیگر را مختل می‌کنند احتمالاً زیاد خطرناک به‌نظر نمی‌رسند، تا چه رسد به اینکه عنوان اعمال جنگی تلقی شوند، اختلال می‌تواند به عظمت تهدیدی امنیتی مانند تخریب باشد.

ناتوان‌سازی، ازکاراندازی و مختل کردن همگی اهدافی مستلزم نوعی درهم شکستن سیستم هستند. در چنین زمینه‌ای، «درهم شکستن» به معنای این است که تمامی منابع از نوع خاصی در خدمت یورشگرند و هیچ‌کدام از آنها را نمی‌توان از دست آن خارج کرد تا در اختیار کاربر قانونی قرار گیرد. مثالی برای این امر، حملهٔ عدم سرویس‌دهی توزیع‌شده[1] است. این حمله، به آسانی سیستم مورد هدف (یا ورودی آن) را درگیر نموده، ارتباطات شبکه‌ای را از کاربرانی که قصد استفاده از آن را دارند جدا می‌سازد. درخواست‌های صورت‌گرفته برای ارتباطات شبکه‌ای توسط یورشگران، تمامی فضای موجود را در صف ارتباطی جذب خود کرده و هرگاه ارتباطی (مثل: سر آمدن وقت) پایان می‌پذیرد، منبعی که از اختصاص یورشگر خارج شد، بلافاصله به آن تخصیص داده می‌شود. اگر ارتباطات شبکه‌ای، غیرمرتبط با حملهٔ عدم سرویس‌دهی توزیع‌شده صورت گیرد، احتمال زیاد موفق نخواهند بود.

وجه دیگر، بستن راه استفاده از منابع است؛ همان‌طورکه در گلولهٔ مرگ، یورشگر، بستهٔ پینگ بسیار بزرگی را ارسال می‌کند. این امر باعث انجماد گیرنده یا قفل شدن منابع آن می‌شود؛ به‌نحوی‌که آنها را برای سایر فرستنده‌ها غیرقابل دسترس می‌نماید. این امر دارای تأثیر یکسانی با درهم شکستن سیستم است؛ ولی یک تفاوت دارد و آن اینکه یورشگر مدام نیاز به ارسال درخواست خود ندارد، بلکه یک درخواست کافی است.

دراین‌صورت حمله یا از ویژگی‌های معلوم هدف بهره‌کشی کرده یا به آسانی منابع را از توان می‌اندازد، که این حاکی از دو ویژگی است: یا حمله ورودی‌های خاصی را برای سد

1. Distributed denial of service attack

کردن منابع به‌کار گرفته یا بارها از منابع استفاده می‌کند. اولین ویژگی در تعیین اولویت مشکل است؛ زیرا ورودی‌هایی که باعث انجماد سیستم می‌شوند، شناخته‌شده نیستند. باوجوداین یورشگر احتمالاً سعی در به‌کار بستن ورودی‌هایی دارد که می‌توانند برخی سیستم‌ها را سد کنند، به امید اینکه یکی از آنها به هدف می‌خورد. دومین ویژگی، افزایش میزان ترافیک است که هدف آن جلوگیری از وجود منابع آزاد در هدف به‌منظور واگذاری به کاربران غیریورشگر است.

نکتهٔ جالب ماهیت این حمله آن است که پس از پایان حمله یا هنگامی که مدیران سیستم منابع را به‌منظور جلوگیری از ارائه هرگونه منبعی به یورشگر، دوباره در اختیار می‌گیرند، سیستم بازیافت می‌شود و این امر آن را از تخریب متمایز می‌سازد؛ زیرا در تخریب، مدیران سیستم باید اقدامات ویژه‌ای را برای بازیافت سیستم صورت دهند. به‌محض‌اینکه حمله مخربی آغاز می‌شود، یورشگر دیگر قادر به اعادهٔ سیستم نیست.

با به‌تأخیر انداختن، تجهیزات به کارکرد خود ادامه می‌دهند، اما آهسته‌تر. گاهی پیغام، به‌طور غیرمنتظره‌ای مدت زمان طولانی‌تری را برای حرکت از نقطه‌ای به نقطهٔ دیگر سپری می‌کند. هدف تأخیر، مختل کردن دریافت به‌موقع پیغام‌هاست. این حمله ممکن است بخش‌های شبکه‌ای فرستنده یا گیرنده یا مسیری را که پیغام باید طی کند، دچار اختلال کند. دو رویکرد اینجا امکان‌پذیر است: یا دستگاه فرستنده یا گیرنده، یا یکی از اجزای شبکه مورد حمله قرار می‌گیرند. در هر دو صورت، حمله مشابه حمله‌ای خواهد بود که به‌منظور ناتوان‌سازی، ازکاراندازی و مختل کردن انجام می‌شود؛ اما باید توجه داشت هدف این نوع حمله، درهم شکستن متناوب سیستم مورد هدف است، تا درهم شکستن آن، تا راه‌اندازی بعدی.

مرز بین ایجاد تأخیر و اختلال، در سرنوشت پیغام‌ها نهفته است. اختلال مستلزم نابودی آنهاست؛ درحالی‌که تأخیر، تنها از رسیدن به موقع آنها جلوگیری به‌عمل می‌آورد. در نتیجه، حملهٔ تأخیرساز تمامی بخش‌های مسیر ارتباطاتی را مختل نمی‌کند، بلکه صرفاً برخی از آنها را دچار اختلال می‌سازد. این نوع حمله محلی‌تر از حملات اخلالگر است و با «ضربه‌ای دقیق» که منابع مهم قابل جایگزینی را ناتوان می‌سازد، قابل مقایسه است؛ اما زمان لازم برای

جایگزینی منابع به‌تأخیر می‌افتد. بنابراین، حملات تأخیرساز دارای ویژگی‌های مشابهی با حملات ناتوان‌ساز، ازکارانداز و مختل‌کننده دارند؛ با این تفاوت که حملات تأخیرساز، به‌جای حمله به کل مسیر، محدود به عناصر خاصی از آن هستند.

انحراف و تحریف، نوعی فریبکاری به‌شمار می‌رود. منطق فریبکاری، ایجاد الگویی است ولو دروغین، که موجب ایجاد تصویری غلط از واقعیت در طرف مقابل است؛ با امید به اینکه او به‌دنبال نتیجه‌گیری خود، یا نادرست عمل خواهد کرد یا از فرصت و موقعیتی که حتی اگر خودش متوجه آن نیست برایش مطلوب است، استفاده نمی‌کند.[1] انحراف یا گمراهی آسان‌ترین و رایج‌ترین شکل فریبکاری است. مکانیسم به‌کاررفته، آرایش نیروهای نظامی خودی، فیزیکی یا الکترونیکی به‌منظور تضعیف توانایی دشمن در متمرکز ساختن منابع و تلاش‌های خود در نقطهٔ معینی جهت دستیابی به پیروزی ناگهانی است.[2] با استناد به گفته سان تزو، پیروزی بستگی به برتری در نقطهٔ معینی از درگیری دارد؛ اما این هدف زمانی بهتر به‌دست می‌آید که تنها بر متمرکزسازی نیروهای خودی تمرکز نشود، آن‌هم درحالی‌که از دشمن غافل باشیم، بلکه لازمهٔ آن، روشی است برای اجبار و دشمن جهت پراکندن نیروها، منابع، قابلیت‌ها و توجه خود. فریبکاری ازطریق انحراف، روزبه روز مهم‌تر می‌شود.[3]

تحریف، شکلی از فریبکاری است که محتوای فضای اطلاعاتی عموم مردم را مورد هدف قرار می‌دهد و اغلب به‌عنوان «مدیریت برداشت‌ها» از آن یاد می‌شود.[4]

---

1. Michael Dewar, **The Art of Deception in Warfare**, Newton Abbot: David & Charles 1989, p. 19.

۲. مثال کلاسیک از فریب دادن به واسطهٔ انحراف عملیات «پایداری سخت» بود که طی آن متحدان در سال ۱۹۴۴ به بخش‌هایی از اروپا حمله کردند. انحراف بر توجه آلمان به (Pas de Calais) و دیگر بخش‌های اروپا متمرکز بود. زمانی که متحدان به نورماندی حمله کردند، آلمان‌ها به مدت تقریباً دو ماه نمی‌دانستند که آیا این حمله، حمله اصلی است یا حمله به Pas de Calais، هدف اصلی بوده است.

3. Michael I. Handel, opcit. p. 159.

4. examines five areas of perception management: lies and distortions, denouncement, harassment, advertising and censorship.

وی، پنج زمینهٔ مدیریت برداشت را مورد بررسی قرار می‌دهد: دروغ‌ها و انحراف‌ها، مردود شمردن، آزار، تبلیغ و سانسور.

ازاین‌جهت تحریف با سایر انواع نبرد اطلاعات که مسیرهای اطلاعات را چه ازطریق تخریب، ناتوان‌سازی، از کاراندازی، مختل کردن یا تأخیر مورد هدف قرار می‌دهد، متفاوت و مستلزم سوءاستفاده از مسیرهای اطلاعاتی یا رسانه‌های ارتباطاتی است، چه درصورت تماس رودررو[۱]، چاپ، مخابرات و ارتباطات از راه دور باشد و چه ازطریق شبکه‌های رادیو و تلویزیونی یا رایانه‌ای.[۲] مکانیسم به‌کاررفته در تحریف، دست‌کاری دقت اطلاعات (به‌وسیله جعل یا دست‌کاری اطلاعات موجود) به‌منظور شکل دادن به برداشت‌های طرف مقابل و ازطریق تأثیرگذاری شدید بر استدلال، تصمیم‌گیری و اعمال آن است.[۳]

درحالی‌که کلاوسویتس از تخریب به‌عنوان اصل اساسی جنگاوری نام می‌برد، سان تزو، فریبکاری را در آن جایگاه والا می‌نشاند؛ زیرا فریبکاری موفقیت‌آمیز، امکان غافلگیر کردن را به انسان می‌دهد. اگر فریبکار بتواند اهداف حقیقی خود را مخفی نگه دارد، دشمن ممکن است نیروهای خود را در جاهای غلط متمرکز و درنتیجه، خود را در نقطهٔ اصلی درگیری تضعیف نماید.[۴]

فریبکاری ارتباط نزدیکی با امنیت دارد. دیور[۵] مقاصد امنیتی را این‌طور بیان می‌کند: جلوگیری از پی‌بردن دشمن به مکان، قابلیت‌ها، نقشهٔ حمله، زمان حمله، ابزار و شیوه‌های حمله و منابع اطلاعات سری.[۶] در مقابل، مقاصد فریبکاری عبارتند از: باوراندن دشمن به اینکه جایی غیر از جای خود هستید، قابلیت‌های شما با آنچه شما هستید تفاوت دارد، نقشهٔ شما این است که کار دیگری، در جای دیگری، در زمان و به روش دیگری به انجام رسانید. فریبکاری موفقیت‌آمیز مشکل به‌دست می‌آید و مستلزم موارد زیر است: کنترل و هماهنگی متمرکز

---

۱ سان تزو مباحثی راجع به بهره‌گیری از مأمورانی که اطلاعات غلط به آنها داده می‌شد و سپس روانه خاک دشمن می‌شدند، عنوان داشته است، به این امید که آنها دستگیر شده و اطلاعات غلط را برای دشمن فاش سازند.

2. Dorothy E. Denning, **Information Warfare and Security**, New York, N.Y.: ACM Press; Harlow: Addison-wesley, 1999. p. 101.

3. Ibid.

4. Michael I. Handel, op.cit., p. 217.

5. Dewar

6. Michael Dewar, op.cit., pp. 18-19.

ازطریق آماده‌سازی، همخوانی با الگویی از رویدادها که دشمن انتظار آن را دارد؛ فزونی (برای مثال، شاخص‌های غلط ارائه‌شده به دشمن ازطریق حداکثر منابع اطلاعاتی سری و تحت نظرگیری)؛ زمان‌بندی دقیق و محتاطانه که به دشمن زمان کافی برای عکس‌العمل نسبت به اطلاعات غلط را بدهد؛ ارائه زمان ناکافی برای تجزیه و تحلیل جهت کشف فریبکاری، و حفظ احتیاط‌های معمول امنیتی به‌منظور برانگیخته نکردن ظن دشمن.[1] دیور تأکید می‌کند که «تمامی فریبکاری‌ها، دورهٔ عمر محدود و نسبتاً کوتاهی پیش از کشف شدن دارند. درجهٔ پیشرفتگی لازم برای موفقیت‌آمیز بودن یک ترفند، به‌طور مستقیم به طول زمان پایداری آن مرتبط است».[2] به‌علاوه افراد، گروه‌ها و جمعیت‌ها در زمینهٔ پذیرا بودن نسبت به فریبکاری متفاوتند. در عصر اطلاعات، آنهایی که به‌شدت بر منابع الکترونیکی و دیجیتالی اطلاعاتی و اطلاعات سری متکی‌اند، به احتمال زیاد، مستعدترین افراد در برابر دست‌کاری و تحریف این نوع منابع اطلاعاتی هستند.

دیور استدلال می‌کند که صحنهٔ جنگ همواره فرصت‌های مشابهی را برای فریبکاری فراهم نیاورده است. در قرن هجدهم، صحنهٔ جنگ کاملاً قابل رؤیت بود؛ لذا بدبینی کلاوسویتس دربارهٔ فریبکاری و غافلگیری صحت داشت. در قرن نوزدهم، صحنهٔ نبرد بسیار بزرگ‌تر شده و

---

1. Ibid., pp. 14-15.

۲. دیور لیستی از تکنیک‌های فریب را ارائه می‌دهد. اولین شیوه عبارت است از تشویق دشمن به اینکه اعتقاد پیدا کند مناسب‌ترین راه برای حصول به هدف آن است که توجه خود را از طرحی جایگزین منحرف سازد. زیرا دشمن تصور می‌کند که فرصت خوبی را به‌دست آورده، درحالی‌که به تله می‌افتد. فرایند تکراری نیز احساس امنیتی غلطی را در دشمن ایجاد می‌کند. بلوف دوگانه نیز دربردارندهٔ افشای حقایق برای دشمن ـ که انتظار فریب را دارد ـ چراکه وی اعتقادی به آن نخواهد داشت، می‌باشد. اشتباه غیرعمومی نیز دشمن را به این اعتقاد می‌رساند که ازطریق نفوذ به سیستم امنیتی و یا غفلت یا ناکارآمدی دشمن، اطلاعات باارزشی را به‌دست آورده است. جایگزینی دشمن را تشویق می‌کند تا چیزی را به اشتباه درک کرده و به‌رغم مشخص شدن واقعیت باز هم به آن تصور غلط ادامه دهد. در واقع می‌توان نیروهای خود را در یونیفرم‌های دشمن پنهان کرد. نهایتاً اینکه، دیور عنوان می‌دارد که تکنیک‌های فریب را می‌توان به لحاظ حس‌ها نیز طبقه‌بندی کرد. استتار دربردارندهٔ فریب بینایی است. از صدا نیز می‌توان برای فریب استفاده کرد.

کمتر قابل رؤیت بود. جنگ جهانی دوم، اوج «صحنهٔ نبرد خالی» بود؛ درحالی‌که فناوری‌های شناسایی و در کنترل داشتن زمان پس از ۱۹۴۵، صحنهٔ نبرد بسیار عظیم‌تری را به رؤیت تقریباً کامل بازگرداند. فناوری‌های دیجیتالی امروزه، به انسان امکان ایجاد و دست‌کاری آسان مدارک و تصاویر دیجیتالی را می‌دهند. صحنهٔ جنگ فیزیکی ممکن است شفاف‌تر باشد؛ اما صحنهٔ نبرد دیجیتالی، فرصت‌های بی‌سابقه‌ای را برای فریبکاری فراهم می‌آورد.

اساس انحراف، جلب توجه دشمن است. درحالی‌که دشمن به کار دیگری مشغول است، یورشگر می‌تواند دست به حملهٔ «واقعی» بزند. این امر باعث شده که انحراف و گمراهی پیش‌درآمد یا بخشی از سایر حملات باشد. این نکته حکایت از یک ویژگی سادهٔ چنین حمله‌هایی دارد: «آشکار بودن». بنابراین حمله باید از نوعی باشد که دشمن بتواند ردیابی کند. دشمن نیز در حالت ایده‌آل، مجبور به انحراف منابع خود برای برخورد با حمله می‌شود. در نتیجه، یورشگر ممکن است از حملات بسیار شناخته‌شده‌ای استفاده کند که نیازمند برداشتن گام‌هایی طبق روال توسط دشمن برای حفاظت در برابر طرف مقابل است. دراین‌صورت دشمن بر حمله متمرکز بوده و ممکن است متوجه حملهٔ ظریف‌تری که حواس او از آن پرت‌شده نشود.

حملات منحرف‌کننده می‌توانند حالت دفاعی نیز داشته باشند. همان‌طورکه در پاسخ انحرافی کلاسیک، در هنگام ورود یورشگران آلمان شرقی به رایانه‌ای در آزمایشگاه لاورنس برکلی[1] در اواسط دههٔ هشتاد صورت گرفت، متصدی سیستم به نام کلیف استال[2]، درصدد ردیابی یورشگرانی برآمد که ازطریق خط تلفن از جایی در آلمان می‌آمدند؛ اما ردیابی تلفن بین‌المللی مستلزم زمان زیادی بود و یورشگر به مدت زمان کافی وصل نبود. بنابراین استال، مدرک اشتباهی را ایجاد کرد که حاوی اطلاعات مطلوبی برای یورشگر بود و بارگزاری[3] این اطلاعات نیز ازطریق خط تلفن چند ساعتی به طول می‌انجامید. زمانی‌که یورشگر مدرک را

---

1. Lawrence Berkeley Laboratory
2. Cliff Stoll
3. Download

یافت، آن را بارگزاری نمود و این امر توجه او را از ردیابی تلفنی که مکان او را مشخص می‌کرد، منحرف کرد.[1]

تحریف، برداشت دشمن را از آنچه در حال رخ دادن است، مدیریت می‌کند. هدف تحریف، باوراندن خواسته یورشگر به دشمن است؛ برای مثال، می‌توان یک سرور پست الکترونیکی را ترتیب داد که به مشتری عبارت «خوش‌آمدی» را با مدل خود (Send mail ۸/۹) بیان کند. این سرور درواقع یک میلر Postfix است و ازآنجاکه سرورهای مختلف پست الکترونیکی دارای آسیب‌پذیری‌های متفاوتی هستند، این امر موجب هدر دادن منابع یورشگر در مقابل حمله‌هایی است که بر سرورهای مدل Send mail ۸/۹ کار می‌کنند و نه بر سرورهای Postfix. به‌طور مشابهی، نیروی هوایی نه‌تنها می‌تواند ارسالات راداری و رادیویی دشمن را کنترل کرده، به آنها ضربه بزند، بلکه می‌تواند اهداف غلط را در رادارهای دشمن بکارد و سیستم‌های دفاع هوایی دشمن را منحرف کند.[2]

یکی دیگر از ویژگی‌های حمله تحریفی، کنترل منابع است. یورشگر باید دسترسی دشمن را به اطلاعات مرتبط با تحریف تحت کنترل درآورد. اگر دشمن به اطلاعاتی دست یابد که نشان‌دهندهٔ عدم هماهنگی باشد، آنگاه متوجه خواهد شد که حمله‌ای در راه است. بنابراین یورشگر باید تمامی راه‌هایی را که دشمن می‌تواند ازطریق آنها اطلاعاتی کسب کند، تحریف نماید و این امر مستلزم درک کاملی از رابطهٔ دشمن با اطلاعات درگیر در تحریف است. این امر نیازمند بررسی نه‌تنها دشمن، که عواملی است که طی مسیرهای جریان اطلاعات وجود دارند تا از عدم کشف تحریف‌ها توسط دشمن مطمئن شوند (و اطلاعات را به دشمن بازخورد دهند).

درحالی‌که تحریف و فریبکاری معمولاً شامل جایگزینی اطلاعات با یک علامت دروغین است، نظارت و کنترل، «نفوذ به فضای اطلاعاتی دشمن و پنهان‌سازی علامت به‌منظور

---

1. Clifford Stoll, "Stalking the Wily Hacker", **Communications of the AGM**, Vol. 31, No. 5, May 1988, pp. 484-97.
2. Thom Shanker and Eric Schmitt, "Firing Leaflets and Electrons, US. Wages Information War", **New York Times,** 24 Feb. 2003, pp. A1, A7.

گردآوری اطلاعات» را دربرمی‌گیرد. نفوذ به‌منظور نظارت، فرصت‌هایی را برای فریبکاری دشمن فراهم می‌آورد؛ زیرا احتمالاً وی از اینکه منابع اطلاعاتی‌اش مورد حمله قرارگرفته بی‌خبر بوده، همچنان بر آنها اعتماد خواهد داشت. نظارت اصل مهمی در فریبکاری است. اطلاعات سری خوب و رسوخ به جبههٔ دشمن از ابزارهای فهم افکار، انتظارات و نقشه‌های دشمن به‌شمار می‌رود.[1]

دراین‌میان تمایز حائز اهمیت، توانایی پیش‌بینی عکس‌العمل‌های دشمن است. با تحریف/ فریبکاری صرفاً گمراهی دشمن چه در فضای اطلاعاتی او یا فضای خودی، و ازطریق تغذیه غلط یا تحریف‌شدهٔ اطلاعات دشمن صورت می‌گیرد. در نظارت/ کنترل تلاش برای مشاهدهٔ کاری است که دشمن درحال انجام آن است و مجبور کردن آن به اعمال یا شرایط خاصی است؛ برای مثال، ممکن است مدارک غلطی را در فضای اطلاعاتی خود قرار داده تا دشمن را گمراه کنیم، اما از نتایج آن خبر نداشته باشیم؛ این تحریف/ فریبکاری است. یا ممکن است مدارکی را تهیه کنیم که منجر به اعمال و نتایج ویژه‌ای شود؛ این کنترل کردن است که فریبکاری بخشی از آن محسوب می‌شود، یا ممکن است سیستم را طوری طرح‌ریزی کنیم که کسانی را که مدارک را دریافت می‌کنند، شناسایی کند؛ این نظارت کردن است.

تفاوت بین نظارت و کنترل این است که نظارت، منفعل و کنترل، فعال است. برای آغاز نظارت ممکن است انجام عملی نیاز باشد؛ اما به‌محض‌اینکه مکانیسم‌های آن به‌راه افتادند، یورشگر دیگر نیازمند اقدام دیگری نیست. در برخی موارد، حمله‌کننده تنها لازم است دشمن را به‌عمل خاصی وادار کند، مثل بارگزاری کردن یک فایل یا اجرای برنامه. تروجان‌ها یکی از مثال‌های این تکنیک هستند.[2]

کنترل کردن مشابه تحریف است؛ اما هدف اصلی آن وادار کردن دشمن به انجام اعمال

1. Michael I. Handel, opcit., pp. 217-S.
2. James P. Anderson, "Computer Security Technology Planning Study", **Technical Report ESD-TR- 73-51, Electronic Systems Division,** Hanscom Air Force Base, Hanscom, MA, 1972.

خاص یا وارد شدن به موقعیت‌های عملیاتی به‌خصوصی است. تحریف ممکن است یکی از اجزای کنترل باشد، همان‌طور که در دست‌کاری برفرد[1] توسط چزویک[2] بوده است.[3] چزویک با تحریف محیطی که برفرد دریافت می‌کرد، او را به انجام اعمال خاصی وادار کرد. او امیدوار بود که برفرد را شناسایی می‌کند.[4]

کنترل ممکن است مستقیم‌تر صورت بگیرد. ابزار حملهٔ نت باس[5,6] به یورشگر اجازهٔ انجام اعمال مدیریت سیستم را می‌دهد؛ اعمالی همچون نظارت بر سایر کاربردهای سیستم، وارد کردن نام کاربر، خواندن صفحه‌های رایانه‌ای و خاموش کردن سیستم. این ابزار در یک بازی رایانه‌ای قرار گرفته بود که در دسترس عموم قرار داشت. برخی از سایت‌ها این بازی را بارگزاری و نصب کرده و درنتیجه به حمله‌کنندگان اجازهٔ کنترل کامل سیستم خود را داده بودند.

نظارت نیازمند توانایی خواندن ترافیک است. این بدان معنی است که یورشگر باید دسترسی خواندن برخی بخش‌های کانال ارتباطی را داشته یا کسب کند. کنترل نیز مستلزم توانایی نوشتن یا جرح‌وتعدیل ترافیک است؛ یعنی یورشگر باید دسترسی نوشتن در برخی قسمت‌های کانال ارتباطی را داشته یا کسب نماید. بنابراین یکی از ویژگی‌های این‌گونه حملات، تحلیل راه‌های ارتباطی مورد استفادهٔ دشمن به‌منظور کسب دسترسی لازم است. دومین ویژگی آن است که حمله‌کننده باید به برخی بخش‌های کانال، ازجمله هسته (یا فرایند ارسال و دریافت) نقطهٔ پایانی، یا یک سیستم رابط رسوخ کند. یورشگر ممکن است به‌طور مستقیم ازطریق حمله‌ای نفوذی، یا غیرمستقیم، توسط یک کرم تروجان که حاوی ضربه به هنگام اجراست، ضربه وارد کند.

---

1. Berferd   2. Cheswick
3. W. Cheswick, "An Evening with Befrerd, in Which a Cracker is Lured, Endured, and Studied", **Proceedings of the 1992 Winter USENIX Conference**, Jan. 1992, pp. 163-173.
4. L. Spitzner, **Honeypots: Tracking Hackers**, Boston, MA: Addison Wesley Professional, 2002.
5. Net Bus
6. Symantec, "Information on Back Orifice and NetBus", <http://www.symantec.com/avcenter/warn/backorifice.html>

۵. اهداف سطح بالاتر

خودنمایی ازنظر سنتی، شامل استفادهٔ صلح‌آمیز از نیروی نظامی برای نشان دادن هیبت خود است. معمولاً ملت‌ها، مهارت‌های نظامی خود را در تمرین‌های نظامی، نمایش‌های ملی یا ازطریق خریداری و تولید سلاح‌های پرستیژی به نمایش می‌گذارند.[1] به عقیدهٔ آرت[2] «کاربرد خودنمایانهٔ نیرو، به‌منظور ارتقای افتخار ملی یا ارضای جاه‌طلبی‌های شخصی حاکم است. یک دولت یا سیاستمدار برای اینکه قدرتمندتر و مهم‌تر جلوه کند، یا دیگران او را در شوراهای تصمیم‌گیری بین‌المللی جدی بگیرند تا تصویر ملت خود را در چشمان آنها ارتقا بخشد، خودنمایی می‌کند».[3] در کوتاه‌مدت خودنمایی هیچ هدف ابزاری خاصی را محقق نمی‌کند؛ اما در بلندمدت ممکن است قابلیت‌های تهاجمی، دفاعی و بازدارندگی کشور را ارتقا دهد. «در دریان»[4] استدلال می‌کند که نمایش‌ها و تمرینات الکترونیکی تأثیرگذار نیز می‌توانند مقصود آزمایش‌های هسته‌ای را تأمین نمایند. خودنمایی قابلیت‌های الکترونیکی خود ازطریق نمایش تکنولوژیکی می‌تواند قدرت را مشهود و تحسین‌برانگیز نماید و درنتیجه به‌عنوان بازدارنده‌ای الکترونیکی عمل کند.[5]

به‌دلیل آنکه خودنمایی، یک عمل عمومی است، یورشگر باید تأثیری برجای بگذارد که قابل رؤیت توسط دیگران باشد. حمله و آثارش، باید برای همه آشکار باشد. یورشگری که به شبکهٔ استنفورد[6] رسوخ نمود، نمونهٔ خوبی از خودنمایی است؛ زیرا او با مدیران استنفورد دربارهٔ کاری که انجام می‌داد، درحین انجام آن صحبت می‌کرد.[7]

ویژگی حملهٔ همراه با خودنمایی مانند هدف آن، قابل رؤیت بودن آن است. لازم نیست نتیجه

---

1. Robert J. Art, **The Four Functions of Force**, New York: Harper Collins, 1996, pp. 159-160.
2. Art
3. Ibid.
4. Der Derian
5. James Der Derian, "Cyber-deterrent", **Wired News**, Vol. 2, No. 9, 2001, pp. 116-122.
6. Stanford
7. B. Reid, Reflections on some Widespread Computer Break-Ins, **Gommunications of the ACM**, Vol. 30, No. 2, Feb. 1987, pp. 103-105.

برای همه قابل رؤیت باشد، ممکن است تنها برای عدهٔ منتخبی این امر صورت پذیرد (مانند مثال بالا)؛ ولی باید حتماً برای کسی قابل رؤیت باشد. بنابراین اهداف مذکور، در اجرا یا نتایج باید آشکار باشند. این امر حاکی از به‌کارگیری تکنیک‌های شناخته‌شده حمله‌ای است که پاسخ‌های کافی برای آن در دسترس نیست تا دشمن بتواند حمله یا نتایج آشکار عمومی را دریابد.

مفهوم مجازات کردن، کاربرد زور برای تحمیل درد و رنج است. شلینگ[1] بین نیروی خشونت‌آمیز که به‌دنبال غلبه کردن بر قدرت دیگری، و تهدید درد که درپی ایجاد محرک در طرف مقابل است، تمایز قائل می‌شود.[2] مجازات، شکلی از احیا است که به‌منظور وادار کردن طرف مقابل جهت متابعت طراحی می‌شود. استفادهٔ موفقیت‌آمیز از استراتژی مجازات مستلزم آگاهی از سرمایه‌ها و نگرانی‌های طرف مقابل است. به عقیده شلینگ، تفاوت بین نیروی خشونت‌آمیز و وادارسازی بیشتر در نیت آنهاست و نه ابزار و شیوه‌ها. نیروی خشونت‌آمیز به‌دنبال ازمیان برداشتن یک مانع نظامی است؛ درحالی‌که کاربرد قدرت برای وادارسازی به‌دنبال اقناع دشمن برای درست رفتار کردن یا تسلیم شدن ازطریق تحمیل درد و رنج شدید و غیرقابل تحمل بر دشمن است. حملات تنبیهی بر مردم نیز می‌توانند در سلسله عملیات گسترده‌تر نظامی جهت مهار کوتاه درگیری مستقیم نظامی به‌کار روند.

ازنظر تاریخی، پیروزی از شکست نیروی نظامی دشمن تا صرفاً صدمه زدن به مردم جهت ازبین بردن طاقت‌ها را دربرمی‌گیرد. تروریسم، محاصره و بمباران استراتژیک ـ که همگی آنها مثال‌هایی هستند از خشونت علیه غیرنظامیان و اساساً به‌منظور وادارسازی صورت می‌گیرند تا تضعیف نظامی دشمن ـ به‌ندرت جهت دستیابی به پیروزی، به‌خودی‌خود مؤثر بوده‌اند. احتمالاً استثنای عمدهٔ این قضیه، بمب‌های اتمی رهاشده بر ژاپن بوده است؛ سلاح‌های ترور و شوک که ارزش آنها در تحمیل درد خالص نهفته است، درست به اندازهٔ تخریب مستقیم نظامی.

---

1. Schelling
2. Thomas C. Schelling, **The Diplomacy of Violence**, reprinted in Art and Jervis, International Politics, pp. 169.

سلاح‌های هسته‌ای نیز امکان تحمیل درد غیرقابل تحمل را بدون دستیابی اولیه به پیروزی نظامی فراهم می‌آورد. معمولاً چنین خشونتی مخصوص اعمال فاتحان بر مغلوبان است. سلاح‌های هسته‌ای نه‌تنها میزان تخریب قابل تحمل، که نقش تخریب را نیز در فرایند تصمیم‌گیری دستخوش تغییر ساخته‌اند.

مجازات، استراتژی‌ای است که نه‌تنها تمایز بین رزمندگان و غیررزمندگان را محو کرده است، بلکه به‌طور مشخص غیرنظامیان را چه طی جنگ و چه پیش از آن، به‌منظور ارعاب، وادارسازی یا بازدارندگی حکومت‌ها مورد هدف قرار می‌دهد.[1] حملات اطلاعاتی بر زیرساخت‌های مهم ممکن است تأثیر مخربی مانند بمب‌گذاری متعارف ایجاد نکنند؛ اما درپی هدف مشابهی هستند؛ اگرچه نتیجهٔ آن ممکن است تنها سرگردانی باشد تا صدمه زدن.

مجازات ازطریق شیوه‌های تکنیکی مستلزم هدف‌گیری سیستم‌های زیرساختی است که استفاده از اینترنت را مختل می‌کند؛ اما به‌دلیل‌آنکه اینترنت هنوز بخش ضروری زندگی مردم نشده، درجهٔ اختلال باید کاربرد آن را برای توزیع محصولات یا خدماتی که برای کارکرد جامعه ضروری‌اند، تحت تأثیر قرار دهد. لذا حملات طراحی‌شده برای مجازات، عرضه‌کنندگان خدمات یا زیرساختار شبکه‌ای را هدف قرار خواهد داد. انواع تکنیکی حملات به‌کاررفته را می‌توان از هریک از مجموعه اهداف تکنیکی فوق استخراج کرد. هدف تکنیکی ویژه‌ای که عظیم‌ترین خرابی را به‌بار آورد، ماهیت حمله را تعیین می‌کند.

بازدارندگی به‌دنبال از جذابیت انداختن حمله است؛ به‌نحوی‌که طرف مقابل اقدام به عملی نکند. این هدف ممکن است ازطریق تهدید به تلافی یا مجازات (آن‌گونه که ذکر شد) یا ازبین بردن احتمال موفقیت یورشگر به‌دست آید. هارکنت[2] مشکل بازدارندگی ازطریق تلافی را به‌خوبی مورد بحث قرار داده، هشدار می‌دهد بازدارندگی در مواقعی که بازیگر غیردولتی آن را آغاز می‌کند، احتمالاً شکست می‌خورد؛ زیرا او می‌تواند گمنامی خود را حفظ کرده و نیز هیچ

---

1. Ibid., p.178.
2. Harknett

جمعیت یا سرمایهٔ مادی برای تحمیل تلافی بر آن نداشته باشد. بازدارندگی با ازبین بردن احتمال موفقیت دشمن می‌تواند شامل ارتقای نیروهای دفاعی خودی علیه حمله، ازطریق امنیت رایانه‌ای نیرومند، یا ناتوان ساختن قابلیت‌های تهاجمی دشمن توسط عملیاتی سرکوبی، طراحی شده باشد و این امر تمامی حملاتی را که تخریب، فاسد یا مختل کرده ، یا ناتوان می‌سازند دربرمی‌گیرد.

درحالی‌که بازدارندگی با هدف بازداشتن دشمن از اقدام به عملی زیان‌بار صورت می‌گیرد، وادارسازی برای تحت فشار قرار دادن وی جهت توقف یا عقب‌نشینی از یک عمل به‌کار می‌رود و می‌تواند درصورت عدم متابعت دشمن از تهدیدات مجازاتی استفاده نماید یا از کاربردهای نمونه یا نمادین نیروی محدود نظامی (جرم، انرژی یا اطلاعات) جهت مجبور کردن حریف به عقب‌نشینی سود جوید.[1] دراین‌راستا باید از زور، دقیقاً به اندازهٔ کافی برای نمایش اراده استفاده کرد و اعتبار کافی برای کاربردهای بعدی آن‌را درصورت لزوم باقی گذارد. اما همان‌طور که جورج[2] می‌نویسد، وادارسازی نیازمند کاربرد زور نیست و ممکن است کاملاً ازطریق دیپلماسی و متقاعدسازی اجرا شود. اگر زور به‌کار برده شود، به‌صورت «ابزار روان‌شناختی پالایش‌شده» در مقابل ابزار بی‌پردهٔ تخریب استفاده می‌گردد. استراتژی وادارسازی، شامل ارتباطات مناسب با طرف مقابل به‌منظور نشان دادن قصد و مذاکره بر سر ضربه‌ای قابل قبول است. حملات نبرد اطلاعات می‌توانند در یک استراتژی وادارسازانه بسیار سودمند باشند؛ زیرا به‌خوبی درجه‌بندی شده‌اند تا ضربهٔ وارده را محدود ساخته، حتی اراده را نشان دهند. استفاده‌های وادارسازانه نبرد اطلاعات نیز مانند خودنمایی کردن، باید قابل رؤیت باشند و تحریف را به حداقل برسانند.

تضعیف مشروعیت و اطمینان، حملاتی را دربرمی‌گیرد که نقاط ضعف دشمن را آشکار

---

1. Alexander L. George, "Coercive Diplomacy: Definition and Characteristics", in Alexander L. George and William E. Simons, ed., **The Limits of Coercive Diplomacy**, Boulder: Westview Press, 1994, p. 10.
2. George

ساخته یا برداشت‌های دیگران را از دشمن تحریف می‌کند.

آشکار ساختن نقاط ضعف ممکن است نیازمند حملاتی باشد که تخریب، ناتوان، فاسد یا مختل می‌کنند. چنانکه در دسترس بودن و اغتنام[1]، از خدماتی است که دشمن در اختیار دارد، به‌تأخیر انداختن نیز می‌تواند هدفی باشد که مشروعیت و اطمینان را تضعیف نماید. گمراهی و منحرف کردن نیز مشروعیت و توانایی دشمن را برای برخورد با حملات تضعیف می‌کند. تنظیم و کنترل ممکن است اعمالی را رو کند که دشمن خواهان سری نگه‌داشتن آنهاست و انتشار عمومی آنها ممکن است موجب دستیابی به هدف اجتماعی شود. همین‌طور کنترل دشمن، به یورشگر امکان مجبور کردن طرف مقابل را جهت انجام اعمالی خلاف بهترین منافع خود، با تضعیف اطمینان و مشروعیت می‌دهد.

تحریف به‌عنوان هدفی در جهت تضعیف مشروعیت و اعتماد دارای دو اثر است: اولین آنها شکلی از کنترل است که در آن دشمن با دیدگاه تحریف‌شدهٔ واقعیت مواجه بوده، درنتیجه عمل نامناسبی را انجام می‌دهد. دومین اثر، تحریف دریافت‌های مشاهده‌گران اعمال دشمن است که منجربه تقبیح دشمن ازسوی آنها می‌گردد. اگر دشمن به‌عنوان «جعبهٔ سیاه» تلقی می‌شود، اولین دیدگاه از کنترل ورودی‌ها توسط یورشگر به‌وجود می‌آید، ورودی‌هایی که دشمن تصمیمات و اعمال خود را بر آن مبنا قرار داده است. اثر دوم از کنترل مسیرهای دشمن بر مشاهده‌گران توسط یورشگر و تحریف خروجی‌های خارج‌شده از وی ظهور می‌کند؛ تفاوت موجود، پاسخ دشمن را تعیین می‌کند: اینکه آیا ورودی‌ها را از سایر منابعی گردآوری نماید که یورشگر نمی‌تواند بر آنها کنترل داشته باشد (و ندارد)، یا اینکه کانال‌های دیگر ارتباط با مشاهده‌گر را پیدا کند.

دست‌کاری بازار هدفی اجتماعی است که از اهداف «الکترونیکی» نظارت کنترل ناشی می‌شود. برای دستیابی به داده‌ها، یورشگر بر دشمن نظارت می‌کند. جهت دست‌کاری بازار،

---

1. Time Liness

یورشگر از داده‌ها برای تعیین اعمال صورت‌گیرنده به‌منظور دستیابی به نتیجهٔ مطلوب استفاده می‌کند. منفعت شخصی ممکن است مستلزم هریک از اهداف «الکترونیکی» برای کمک به دستیابی هدف موردنظر توسط یورشگر باشد؛ درنتیجه ویژگی‌ها و پیش‌درآمدهای آن اهداف الکترونیکی، منجربه این هدف اجتماعی خواهند شد.

در هر حال در یک جمع‌بندی می‌توان گفت رویکرد ما به فهم پویایی نبرد اطلاعات بر پایه اعتقاد به اینکه تجزیه و تحلیل «حمله ـ محور» بر تجزیه و تحلیل «اثر ـ محور» برتری دارد، بنا شده است. فهم آثار حملات، جهت بازیافت حائز اهمیت است؛ اما دفاع علیه نبرد اطلاعات در مرحلهٔ اول مستلزم فهمی از احتمال انواع مختلف حمله است و تمامی حملات به‌طور برابر محتمل یا قابل اجرا توسط همهٔ انواع حمله‌کنندگان نیستند و سیستم‌ها نیز ازنظر آسیب‌پذیری در برابر همهٔ انواع حملات، یکسان نیستند. انتخاب نوع حمله نیز به روشی نظام‌مند مبتنی‌بر نوع یورشگر (مثلاً دولت، بازیگر غیردولتی یا فرد) تفاوت خواهد کرد؛ زیرا انواع مختلف بازیگران احتمالاً دارای انگیزه‌ها، قابلیت‌ها، انطباق‌پذیری و افق‌های زمانی متفاوتی هستند.

لذا تجزیه و تحلیل حمله ـ محور دارای پتانسیل تشخیصی است. نوع حملهٔ صورت‌گرفته ما را از انگیزه‌ها و قابلیت‌های یورشگر آگاه ساخته و نشان‌دهندهٔ فهم او از آسیب‌پذیری‌های هدف است. شباهت‌هایی باید میان پویایی‌شناسی جنگاوری در حوزه‌های نظامی و تجاری وجود داشته باشد که در گذشته وجود نداشتند؛ زیرا کارآفرینان و جنگاوران، دارای نیازهای مشابهی در زمینهٔ سیستم‌های اطلاعات هستند؛ از قبیل آنکه آن سیستم‌ها ارتجاعی بوده و بتوانند در شرایط عدم قطعیت حاصل از خطاهای انسانی، ناتوان شدن سیستم یا حملهٔ بدخواهانه درست عمل کنند. بااین‌حال یورشگرانی که برای یک حکومت کار می‌کنند، احتمالاً نوع حملات متفاوتی را از یورشگرانی که برای یک شرکت کار می‌کنند، صورت خواهند داد؛ زیرا اهداف و آموزش آنها به‌طور قابل ملاحظه‌ای متفاوت است.

از دیدگاه حمله ـ محور می‌توان گفت که به‌رغم تأثیر هم‌تراز فناوری اطلاعات، دولت‌ها و گروه‌های حمایت‌شده توسط دولت، امتیازات مشخصی را در نبرد اطلاعات کسب خواهند

نمود. عقیدهٔ رایجی وجود دارد که می‌گوید فناوری اطلاعات قلمروهای یورشگران را هم‌سطح کرده و این امکان را فراهم آورده است که یک فرد بتواند ویرانی عظیمی پدید آورد؛ کاری که پیش‌ازاین تنها در حوزهٔ امکان دولت‌ها و سازمان‌هایی با مقادیر عظیمی از منابع امکان‌پذیر بود. حملات به‌کار رفته ممکن است یکی باشند، مجموعهٔ حملات در اینترنت برای کاربرد افراد و دولت‌ها در دسترس باشد و فرد بتواند به تنهایی خرابی عظیمی به‌بار آورد؛ اما برابر دانستن یک یورشگر تنها با دولت‌ها و سازمان‌های مشابه، سه مؤلفه را نادیده می‌انگارد: سازمان‌دهی، اطلاعات سری دربارهٔ هدف و پایداری.

نخست‌اینکه حمله حمایت‌شده توسط دولت به یورشگران امکان سازمان‌دهی بهتری می‌دهد. چنانچه دفاع‌کنندگان در برابر حمله مقاومت کنند، یورشگران دولتی می‌توانند به‌سرعت ارسال بسته‌ها را به‌منظور درهم شکستن مانع جدید افزایش دهند؛ درحالی‌که یک یورشگر تنها، یا گروهی از حمله‌کنندگان سست سازمان‌دهی‌شده، توانایی پاسخ سریع یا مؤثر به دفاع صورت‌گرفته را ندارند. یورشگران دولتی دارای مزیت منابع، توانایی‌های ارتباطی قوی‌تر و حمایت از برنامه‌ریزی هستند که به آنها امکان تخمین دفاع‌ها و برنامه‌ریزی کردن ضد آنها را می‌دهد.

دوم، درحالی‌که ابزار حمله قابلیت‌های دست زدن به آن را تأمین می‌کند، دانش استفادهٔ مؤثر از حملات را ارائه نمی‌نماید. یورشگر تنها ممکن است بتواند برخی از ابزار حمله را به‌طور مؤثر به‌کار بندد، اما گروهی سازمان‌دهی‌شده که می‌تواند از طیف گستردهٔ تجربیات و دانش اعضای گروه استفاده کند، توانایی شناخت کاربرد مؤثر ابزار حمله و چگونگی استفاده از آنها را برای رسیدن سریع به هدف خواهد داشت. اگر حمله‌کنندگان منابعی را در خارج از گروه داشته باشند، که چه بهتر؛ به‌خصوص اگر امکان یادگیری دربارهٔ سازمان‌دهی هدف خود و قابلیت‌های پاسخ‌دهی آن برایشان فراهم باشد. به‌علاوه در عرصهٔ تکنیکی، یورشگران می‌توانند علیه سیستم‌ها، شبکه‌ها و روال‌های سازمانی دشمن تمرین کنند؛ درست مانند زمانی‌که نظامیان حرفه‌ای هنر جنگ را در موقعیت‌های آموزشی تمرین کرده‌اند تا بتوانند

سریع‌تر به هدف مورد نظر خود برسند. این در صورتی است که یورشگر تنها توانایی این کار را ندارد.

سوم، مؤثر بودن حمله یکی از کارکردهای ضروری برای پایداری آن است. زمانی‌که فرد دست به حمله می‌زند، به منابع محدودی دسترسی دارد؛ اما هنگامی که دولت حمله‌ای را حمایت می‌کند، یورشگران دارای منابع (و پول) بیشتری هستند؛ برای مثال، حملهٔ گروهی حمایت‌شده توسط دولت می‌تواند در برابر کشف و دخالت پایدار بماند؛ زیرا به‌راحتی می‌توانند ریشهٔ حمله را به جایگاه جدیدی منتقل کنند؛ درحالی‌که یورشگر تنها، به‌محض اینکه گرفته شود، دیگر نمی‌تواند چنین کند.

بررسی‌های فوق، نه‌تنها دربارهٔ حملات حمایت‌شده توسط دولت، بلکه درخصوص حملاتی نیز که از موجودیتی غیردولتی با منابع و توانایی سازمان‌دهی سر می‌زند، صدق می‌کند. حمله کردن می‌تواند فعالیت فردی یا گروهی باشد؛ اما ملزومات اساسی سلسله عملیات در جنگاوری که در گذشته وجود داشته‌اند، در بنیاد تغییر نکرده و تنها به عرصه‌ای جدید وارد شده‌اند.

فصل چهارم
اشکال و ابزار نبرد اطلاعات

- اشکال نبرد اطلاعات
- جنگ C4I
- ابزارهای جنگ اطلاعات

۱. اشکال نبرد اطلاعات

نبرد اطلاعاتی را می‌توان به اشکال مختلف تقسیم‌بندی نمود؛ اما به‌نظر می‌رسد طبقه‌بندی زیر از انواع دیگر کارآمدتر باشد:[۱]

۱. جنگ C_4I[۲]؛

۲. جنگ مبتنی بر اطلاعات ـ عملیات؛

۳. جنگ الکترونیکی؛

۴. جنگ روانی؛

۵. جنگ ادراکی؛

۶. جنگ سایبر.

۱ـ۱. جنگ C_4I

مفهوم C_4I از چهار C پدید آمده است: فرماندهی، نظارت و کنترل، رایانه و ارتباطات.

هدف این جنگ جدا کردن مسیر ساختار فرماندهی دشمن از بدن نیروهای تحت فرمان است. بی‌سر کردن ممکن است با وارد کردن ضربه به سر یا بریدن گردن صورت گیرد که

---

۱. برای مطالعه بیشتر درخصوص انواع جنگ‌های اطلاعاتی به منبع زیر مراجعه شود

Martin C. Libicki, **What is Information Warfare?**, Washington. D.C.: Center for Advanced Concepts and Technology Institute for National Strategic Studies, National Defense University, 1995.

2. Command Control, Computer and Communication Warfare

هرکدام در خدمت اهداف تاکتیکی و استراتژیک متفاوتی قرار دارند.[۱]

● **عملیات ضدسر**[۲]: شلیک کردن به سر فرماندهی، یک جنبه قدیمی جنگ است. در گذشته همواره این نوع عملیات بر حذف فیزیکی فرماندهان عالی جنگ متمرکز بوده و به‌طورکلی حذف آنها تأثیرات قابل توجهی بر نتایج جنگ داشته است. امروزه علاوه‌بر اهمیت نقش فرماندهان مراکز فرماندهی به‌عنوان مؤلفه‌ای بسیار مهم در عملیات ضدسر ایفای نقش می‌کند.

مراکز فرماندهی زمان ما، با ارتباطات زیاد و محسوس و درگیر بودن رایانه‌ای و الکترومغناطیسی و رفتارهای متمایز که این محل‌ها را از سایر محل‌های نظامی متمایز می‌کنند تشخیص داده می‌شوند. حمله به یک مرکز فرماندهی، به‌ویژه اگر به‌موقع انجام گیرد، می‌تواند حتی بدون زدن یک فرمانده عالی‌رتبه دشمن، عملیات را مختل کند.

دراین‌میان بمب‌های فلزی تنها راه حمله به مراکز فرماندهی نیست. می‌توان با قطع برق، استفاده از دخالت الکترومغناطیسی تا حدی که استفاده از دستگاه‌های الکترومغناطیسی را غیرقابل اعتماد کند و وارد کردن ویروس رایانه‌ای، سیستم‌ها را از کار انداخت. اما هیچ‌کدام از وسایل، در مقایسه با ریختن بمب بر هدف، ازنظر هزینه ـ منافع مقرون‌به‌صرفه نیست. اگرچه پاره‌ای از این اقدامات در مقایسه با مهمات متعارف، بر شعاع بیشتری اثر می‌گذارند، تفاوت، محدود است و پیدا کردن قبل از آتش کردن، همچنان اساسی است.[۳]

● **عملیات ضدگردن**[۴]: این عملیات علیه خطوط ارتباطی و اطلاعاتی فرماندهی و بخش‌های مختلف صحنه عملیات صورت می‌گیرد و هدف آن ارتباطات الکترونیکی صحنه

---

۱. برای مطالعه بیشتر درخصوص نقش اطلاعات در نبردهای اطلاعاتی استراتژیک، تاکتیکی و عملیاتی، مراکز ثقل بنیان‌های نظامی، سیاسی، اجتماعی و اقتصادی دشمن می‌توان از منبع زیر استفاده کرد:

USAF, Air Force Doctrine Document-5 (1st draft), Nov. 1995, 20.

2. Antihead

3. George J. Stein, "Information War-Net War-Cyberwar", in B. R. Schneider and L. E. Grinter, eds., **Battlefield of the Future: 21st Century Warfare Issues,** Maxwell AFB, Alabam: Air University Press, 1995.

4. Antineck

عملیات است.

سازمان‌ها و رده‌های مختلف ارتش‌های مدرن از اواسط قرن نوزدهم به‌وسیله ارتباطات الکتریکی و از دهه بیست با مخابرات رادیوالکترونیکی به‌هم مرتبط شده‌اند. اگر این ارتباطات قطع گردد، فرماندهی و کنترل فلج می‌شود. آنچه جدید است، زیاد بودن ارتباطات در عصر اطلاعات است؛ برای مثال، سیستم‌های دفاع هوایی، درحالی‌که به‌صورت یکپارچه کار می‌کنند، در مقایسه با حالتی‌که هر دستگاه، مستقل عمل می‌کند، کارایی بیشتری دارند.

برای قطع پیوندهای ارتباطی لازم است معلوم باشد که طرف دیگر به چه میزان ارتباط برقرار می‌کند. اگر معماری ارتباطات آن بر تلگراف زدن مبتنی است، دراین‌صورت گره‌ها را می‌توان مورد شناسایی قرار داد و از کار انداخت.[1] سیستم‌های مخابراتی را نیز می‌توان مانند مراکز فرماندهی، با حمله به ژنراتورها، پست‌های برق و خطوط لوله‌های سوخت (مانند خط لوله گاز که به نیروگاه گاز می‌رساند) از کار انداخت. اگر معماری بر الکترومغناطیس استوار است، معمولاً گره‌های اصلی (مثل برج‌های مایکروویو) قابل مشاهده نیستند. اگر برای ارتباطات و ارسال سیگنال‌ها از ماهواره استفاده می‌شود، بر روی خط مخابرات می‌توان پارازیت وارد کرد یا آن را از کار انداخت.

اثر حملات بستگی به این دارد که طرف مقابل تا چه حد در سیستم‌های رایانه‌ای پیشرفت کرده باشد. یک شبکه رایانه‌ای مرکب از تعداد زیادی رایانه‌های کوچک (به‌جای یک یا دو رایانه بزرگ) امواج کمتری منتشر می‌کند و سایه کوچک‌تری می‌اندازد. این شبکه‌ها، کانال‌های موازی[2] بیشتری عرضه می‌کنند و مشکلات هدف‌گیری دشمن را بر هم انباشته می‌سازند. سیستم‌هایی که ترافیک پیام را تکرار می‌کنند، این احتمال را که پیامی در شرایط بسیار بد ارسال شود، چند برابر می‌کنند. سروصداهای اضافی را می‌توان با فناوری‌های جدید مانند

---

۱. مانند هجوم به ساختمان AT & T در بغداد توسط هواپیماهای آمریکایی

2. Redundancy

پخش ـ طیف[1] که در برابر خطای انفجار در محیط فوق‌العاده پر ترافیک و تکنیک‌های پیشرفته اصلاح خطا عمل می‌کنند، محافظت کرد.

نفوذ بالقوه جنگ فرماندهی و کنترل بر نتیجه نبرد، در معماری روابط فرماندهی در نیروی مورد حمله حائز اهمیت است. ساختار، فرهنگ سازمانی و استراتژی‌های نظامی کشوری که در معرض عملیات C4I قرار گیرد، در نتیجه عملیات بسیار مهم هستند. در این چارچوب چنانچه سازمان نیروهای مدافع کاملاً سلسله مراتبی، تابع دستورات مقامات مافوق و فاقد ابتکار عمل باشد، در برابر عملیات C4I آسیب‌پذیرتر است.

۱ـ۲. جنگ مبتنی‌بر اطلاعات ـ عملیات[2]

جنگ مبتنی‌بر اطلاعات ـ عملیات زمانی انجام می‌گیرد که اطلاعات کسب‌شده از دشمن، به‌طور مستقیم به عملیات تزریق شود، نه اینکه به‌عنوان یک داده به فرماندهی و کنترل منتقل و مورد استفاده قرار گیرد. جنگ مبتنی‌بر اطلاعات ـ عملیات، برخلاف جنگ‌های سایبر به‌طورمستقیم به کاربرد فولاد علیه دشمن (نه بایت‌های خراب‌شده) منجر می‌شود.

این جنگ از تغییر در آنچه اطلاعات ـ عملیات برای آن مفید است خبر می‌دهد. معمولاً فرمانده از اطلاعات عملیاتی برای سنجش وضعیت، موقعیت و مقاصد کلی طرف دیگر استفاده می‌کند. هدف از اطلاعات ـ عملیات جلوگیری از غافلگیری و قادر ساختن فرمانده به تهیه نقشه‌های جنگی است. اهداف این عملیات زمانی برآورده می‌شود که در هنگام جنگ یک طرف وظایف خود را درک کرده و آماده انجام آن است، ولی طرف دیگر از گیجی و یکه خوردن دور خود می‌چرخد.

به‌تدریج که دریافتگرها (سنسورها) دقیق‌تر و قابل اعتمادتر می‌شوند، نوع و تعداد آنها افزایش می‌یابد و قادر می‌شوند در زمان واقعی یا نزدیک به زمان واقعی سیستم‌های کنترل

1. Spread-Spectrun
2. Intelligence-Base Warfare (IBW)

آتش را تغذیه کنند. وظیفه ایجاد، نگهداری و بهره‌برداری از سیستم‌هایی که میزان جنگ را حس می‌کنند، ترکیب آن را ارزیابی و نتایج را به شلیک‌کننده ارسال می‌کنند، برای ارتش‌های فردا اهمیت روزافزون می‌یابد. نبرد اطلاعات ـ عملیات را به شرح زیر می‌توان به دو نوع کلی تقسیم کرد:

● **جنگ تهاجمی مبتنی‌بر اطلاعات ـ عملیات:**[1] افزایش سریع نسبت قدرت به قیمت فناوری‌های اطلاعات، به‌ویژه اطلاعاتی که بر سیستم‌های توزیع‌شده مبتنی است، نشان می‌دهد که برای جمع‌آوری و توزیع اطلاعات، معماری‌های تازه‌ای لازم است. محیط میدان‌های جنگ فردا شامل معماری مخلوطی از تعدادی دریافتگر (سنسور) خواهد بود که در سطوح مختلف پوشش قرار دارند و میدان جنگ را به‌طور کامل نشان می‌دهند. براین‌اساس دریافتگرها را می‌توان به چهار دسته کلی به شرح زیر تقسیم کرد:

الف. دریافتگرهای قرارگرفته در دور (به‌طورکلی دریافتگرهای فضایی، ولی شامل دریافتگرهای لرزشی و اکوستیک نیز هست)؛

ب. دریافتگرهای قرارگرفته در نزدیک (مثل: هواپیماهای بدون سرنشین با دستگاه‌های رادار و توانمندی‌های جاسوسی الکترونیک که درضمن به شناورها و رادار زمینی نیز مجهزند)؛

ج. دریافتگرهای واقع در محل (مثل: دریافتگرهای اکوستیک، گرانی‌سنج، زیست شیمیایی)؛

د. دریافتگرهای سلاح (مثل: مادون قرمز، رادار انعکاسی و نوریاب).

این تنوع دریافتگرها، بزرگی و پیچیدگی کار کسانی را که می‌کوشند از نظارت دقیق بگریزند نشان می‌دهد. باوجوداین از تکنیک‌هایی مانند: دود، رنگ منحرف‌کنندهٔ رادار و ساکت‌کننده برای عبور از دریافتگرها استفاده می‌شود.

● **جنگ تدافعی مبتنی‌بر اطلاعات ـ عملیات:** وضعیت دیگری که به همان اندازه، پیش‌بینی و تدارک آن مشکل است، ایجاد روشی دفاعی به‌منظور افزایش شکاف میان تصویر و

---

1. Offensive IBW

واقعیت در میدان جنگ است. ازیک‌طرف برخی کشورها مصمم هستند علیه هواپیماهای دریافتگر (مانند آواکس) عمل نمایند و ازطرف‌دیگر، استفاده از دریافتگرهایی که ارزان‌تر از سلاح‌های مهاجم هستند، عاقلانه‌تر است (یعنی پرتاب یک موشک ده‌هزار دلاری برای زدن دریافتگر هزار دلاری منطقی نیست). به دریافتگرها می‌توان با ازکار انداختن سیستم‌های مورد استفاده آنها (یعنی نفوذ به سیستم‌های کامپیوتری) حمله کرد و سیستم‌های آنها را خراب نمود یا بر آنها سوار شد (یعنی جنگ الکترونیکی).

جالب‌ترین دفاع، در خصوص دشمن احتمالی در ده یا بیست سال آینده، استفاده از نوعی پوشش سنتی (استتار) و فریب دادن با ترکیبی از شگردهاست. وقتی آنچه از دریافتگرها به‌دست می‌آید ازنظر تکنیکی درست باشد (یعنی، آنچه خوانده می‌شود منعکس‌کننده واقعیت باشد) لازمه خنثی کردن جنگ تدافعی مبتنی‌بر اطلاعات عملیاتی این است که پیوندهای بین آنچه دریافتگر می‌خواند و آنچه سیستم دریافتگر محاسبه می‌کند منحرف شود.

در مناطق پرتراکم (مثل: مناطق شهری، روستاهای پرجمعیت، جنگل‌ها، کوه‌ها، و آب‌های گل‌آلود) ضداستراتژی‌ها ممکن است بر استفاده یا دست‌کاری در محیط استوار باشند. در مناطق با چگالی کم (مثل: دشت‌ها، صحراها، دریاها و اقیانوس‌ها)، یک شیء ساخت انسان، به‌ویژه شیء نظامی، به‌صورت چیزی که به آنجا تعلق ندارد مشخص می‌شود و لذا برای اینکه هدف نباشد باید به پیرامون خود شبیه باشد. در مناطقی که خدمات و تجهیزات عمومی و غیرنظامی فراوان است، تجهیزات نظامی باید طوری انتخاب شوند که با تجهیزات غیرنظامی اشتباه شوند. برای این کار، باید تعداد آنها زیاد باشد، کمتر به‌طور مستقیم به تلاش جنگی مربوط باشد و هدف ارزشمندی نباشد.

در عالم نظری، پنهان کردن یک درخت در جنگل بسیار عملی‌تر از محصور کردن آن با دیوار آجری است. موفقیت این اقدامات، با معماری سیستم‌های جنگ مبتنی‌بر پنهان‌کاری که برای فریب دادن طراحی شده، تغییر می‌کند. فریب دادن سیستم‌های مبتنی‌بر دریافتگرهای چندگانه و متداخل مشکل‌تر از فریب دادن سیستم‌های تک دریافتگر است.

۱ـ۳. جنگ الکترونیکی[1]

جنگ الکترونیکی برای کاهش دادن ارتباطات، چه در سطح فیزیکی (ازطریق پارازیت در رادارها یا مخابرات) و چه در سطح ترکیبی (به‌وسیله رهگیری یا حقه زدن) انجام می‌شود.[2]

- **ضدرادار:**[3] بخش بزرگی از جنگ الکترونیکی به رادارها (چه برای جست‌وجو و چه به‌عنوان هدف) و نگرانی در مورد امواج پارازیت و ضد آنها مربوط می‌شود. امروزه برای ازکار انداختن رادار، پارازیت‌انداز باید به دریافت سیگنال ورودی، تعیین فرکانس آن، ایجاد سیگنال پارازیت خروجی مطابق با آن با سرعتی که برای به‌حداقل رساندن طول و قدرت سیگنال منعکس شده است متوسل شود. هواپیمای پارازیت‌انداز که با هواپیمای مهاجم پرواز می‌کند، اغلب با بیش‌ازحد نیرو دادن به سیگنال‌های برگشت آنها را پاک می‌کند.
- **ضدمخابرات**[4]: جنگ الکترونیکی علیه مخابرات معمولاً مشکل‌تر از جنگ الکترونیکی علیه رادارهاست. قدرت سیگنال‌های مخابراتی با نرخ مجذور فاصله آن تا فرستنده ضعیف می‌شود. درحالی‌که رادار می‌کوشد هدف را فعال کند (و بنابراین به رادارهای طرف دیگر، پرتو بیندازد)، در مخابرات سعی می‌شود به‌طور کلی از طرف دیگر اجتناب گردد و لذا رو به جهات مشخص دارد.
- **رمزی‌نگاری**[5]: هر دو طرف پیام‌های خود را به‌نحوی‌که فقط برای خود آنها قابل درک باشد مخابره می‌کنند و درعین‌حال سعی در درک پیام‌های طرف مقابل دارند. با این کار، آنها نمونه کامل یک اقدام نبرد اطلاعاتی را نشان می‌دهند و در عین مختل کردن دید طرف دیگر از واقعیت، دید خود را از واقعیت حفظ می‌کنند. اگرچه رمزی‌نگاری همچنان بهترین مغزهای ریاضی را جذب می‌کند، مجادلات این قلمرو به‌زودی فقط

---

1. Electronic Warfare

۲. جنگ الکترونیک به‌صورت مبسوط در مقاله‌ای جداگانه در همین کتاب آمده است.

3. Antiradar
4. Anticommunications
5. Cryptography

علایق تاریخی را برخواهد انگیخت.

گشودن رمز پیام‌های ایجادشده توسط رایانه، به‌سرعت به‌سوی غیرممکن شدن پیش می‌رود. ترکیب فناوری‌هایی مانند: استاندارد سری‌سازی سه رقمی (DES) که مخصوص مخابره پیام با کلیدهای خصوصی است و سری‌سازی کلید عمومی (PKF) که مخصوص گذشتن از کلیدهای خصوصی با استفاده از کلیدهای عمومی است، احتمالاً بهترین رایانه‌های رمزشکن را شکست خواهد داد.

۱ـ۴. جنگ روانی[1]

جنگ روانی به مفهومی که ما در اینجا به‌کار می‌بریم، از اطلاعات علیه انسان‌ها استفاده می‌کند نه علیه رایانه‌ها[2] و عبارت است از:

- عملیات علیه اراده ملی؛ استفاده از جنگ روانی علیه اراده ملی یا ازطریق «دستکش مخملی» (ما را به‌عنوان دوست خود بپذیرید) یا مشت آهنین و همچنین استفاده از روش‌های روانشناختی علیه نیروهای طرف مقابل صورت می‌گیرد.
- عملیات علیه فرماندهی دشمن؛
- عملیات علیه نیروهای نظامی؛
- جنگ فرهنگی.

هیچ‌چیز به‌اندازه فرماندهان گیج‌شده و دستپاچه، از شکست قریب‌الوقوع خبر نمی‌دهد. گیجی و دستپاچگی، حالت‌های شناختی و درعین‌حال عاطفی هستند. فرماندهان براساس رویدادهای غیرمنتظره تصمیم می‌گیرند. اگر واقعیت با آنچه مبنای تصمیم‌گیری آنها بوده فرق داشته باشد، بازسازی یک ساختارشناختی، مشکل و وقت‌گیر خواهد بود. شبیه‌سازی، تجربه فکری و تفکر

1. Psychological Warfare

۲. جنگ روانی یکی از مقولات اصلی جلد چهارم، مجموعه کتاب‌های جنگ نرم است و در آنجا به شکل مبسوط درباره آن توضیح داده خواهد شد.

تعمیم داده‌شده «چه می‌شود اگر...» ـ که می‌تواند فرمانده‌ای را آماده شناختن دامنه وسیعی از گزینه‌ها (و منطق تصمیم‌گیری هریک از آنها) کند ـ از عهده اتفاقات غیرمنتظره بر آمدن را تسهیل می‌کند، اما به قیمتی گزاف. اندیشیدن به جور کردن (ردیف کردن) ممکن‌ها، لزوماً مانع اندیشیدن عمیق به محتمل‌ها می‌شود. رویدادهایی که احتمال وقوع آنها کم است، به‌طورکلی کنار گذاشته می‌شوند. درنتیجه اگر رویدادهای اخیر روی دهند، عده کمی می‌توانند از عهده آنها برآیند.

جنگ روانی همچنین می‌تواند به فعالیت روزانهٔ فریب دادن دستگاه‌های اداری دشمن (بعضی دیپلمات‌ها و جاسوسان) در زمینه نیات و توانمندی‌ها معطوف شود. می‌توان سلاح‌ها را کمابیش کارآمدتر از آنچه واقعاً هستند جلوه داد. آمادگی‌های یک کشور برای جنگ را می‌توان به‌دلیل اهمیت دادن به اثر آن برجسته کرد یا برای فریب دادن، کمتر از واقع نشان داد. این نوع فعالیت به‌حدی رواج داشته، در تاریخ سابقه دارد که جنگ نامیدن آن (به جای کارهای روزمره نامیدن آن) همواره مشکل بودن خود را ثابت کرده است.

۱ـ۵. جنگ ادراکی

جنگ ادراکی جنبه‌ای از نبرد اطلاعاتی است که تبعات احتمالی نگران‌کننده‌ای درپی دارد[1] و عبارت است از «عملیات‌هایی که به‌منظور تأثیرگذاری بر عقاید و رفتار مردم، از رسانه‌های جمعی در دسترس آنها سوءاستفاده می‌کنند».[2] جنگ ادراکی هدفی مشابه عملیات روانی[3] دارد؛ اما حوزه عمل آن از حوزه عمل عملیات‌های روانی گسترده‌تر است. عملیات‌های روانی قصد دارند تا بر انگیزه دشمن در پی‌گیری مقاصد نظامی تأثیر بگذارند؛ اما هدف جنگ ادراکی این است که ارزش‌ها، ادراکات و اهداف ملی را دست‌کاری کنند. جنگ ادراکی با دیپلماسی علنی

---

۱. درخصوص جنگ ادراکی در کتاب جنگ نرم ۴ به‌طور مبسوط بحث خواهد شد.

۲. نبرد اطلاعاتی به حضور فیلسوفان، مردم‌شناسان فرهنگی، متخصصان موضوعی، زبان‌شناسان و معناشناسان نیازمند است. دوران عدم توجه کالج‌های جنگ یا کارکنان آنها به مفاهیم و موضوعات دیگر گذشته است.

3. psy-ops

و عمومی ارتباط پیدا می‌کند؛ اما این دو مسئله، یکی نیستند. دیپلماسی علنی دولت به روابطی منجر می‌شود که در آن مقاصد سیاست خارجی پی‌گیری می‌شود. در فرایند دیپلماسی، موضوعی که برای یک طرف دارای منفعت است، برای طرف دیگر مطرح، و سعی می‌شود تا او نسبت به آن موضوع متقاعد گردد. دیپلماسی علی‌القاعده شامل دروغ و فریب نیست؛ اما دروغ و فریب از عناصر اصلی فرایند مدیریت ادراکی محسوب می‌شوند. درحقیقت هدف جنگ ادراکی این است که یک طرف، دیگری را به باور کردن چیزی متقاعد کند که خود می‌خواهد، حال حقیقت «هر چه می‌خواهد باشد».

پیش از وقوع انقلاب اطلاعات، جنگ ادراکی به‌طورعمده بر «عملیات‌های روانی» تأکید داشت و روش‌های مورد استفاده آن عبارت بودند از: پخش اعلامیه ازطریق هواپیما یا پخش برنامه‌های رادیویی. هم‌اکنون هراندازه که دشمن به عصر اطلاعات وارد شده باشد، به‌همان اندازه امکانات نبرد اطلاعاتی علیه وی وجود دارد و درعین‌حال تکنیک‌های کنونی نیز نسبت به گذشته کاراتر شده‌اند. اگر مالکیت تلویزیون به امری همگانی تبدیل شود، آنگاه تأثیرگذاری بر ادراکات جامعه یا نخبگان آن ازطریق دست‌کاری تصاویر تلویزیونی امکان‌پذیر است. استفاده گسترده از ماشین‌های دورنگار نیز امکانات بیشتر و درعین‌حال محدودتری را دراین‌زمینه فراهم می‌کند. در جامعه‌ای که از اینترنت استفاده می‌کند نیز فرصت‌های انجام جنگ ادراکی فراهم است: سایت‌های اینترنتی گسترده‌ای ایجاد خواهند شد که اطلاعات گمراه‌کننده و مطلوب دشمن را در اختیار افراد قرار می‌دهند؛ این مسئله به‌معنای دسترسی به سایت‌های دیگران و همکاری با آنها نیز هست.[1] فناوری دیجیتال امکان ایجاد تصاویر جعلی را فراهم آورده است؛ تصاویر جعلی که کاملاً واقعی و حقیقی به‌نظر می‌رسند، از جمله تصاویری از افراد شرکت‌کننده در فعالیت‌ها یا سخنرانی‌های جعلی و ساختگی. یکی از نظریه‌پردازان نبرد اطلاعات این سؤال را مطرح می‌سازد:

---

1. John R. Boyd, **Briefing slides, subject: A Discourse on Winning and Losing,** Maxwell AFB, Alabam August 1987.

آیا کسانی که گفت‌وگوی تام هنکس و جان اف. کندی را در فیلم «فارست گامپ» دیده‌اند، می‌توانند در مورد ایجاد نوار ویدیویی ساختگی از رهبری دشمن که درحال توهین به مقدسات دینی و فرهنگی است، تردید به خود راه دهند؛ نواری که به‌منظور بی‌ثبات ساختن یک رژیم ساخته شده است... در این زمانه که چشمان انسان به آسانی فریب می‌خورند چگونه می‌توان به ضرب‌المثل «شنیدن کی بود مانند دیدن» (تا چیزی را ندیده‌ای، باور نکن) اعتماد کرد؟[1]

جنگ ادراکی، دو نگرانی ایجاد می‌کند: نگرانی نخست اینکه ممکن است ابزار اجرای این نوع از جنگ به‌منظور جلب حمایت از سیاست ملی به درون جامعه تغییر مسیر دهد. این مسئله از تهدیدی جدی برای امنیت ملی خبر می‌دهد؛ تهدیدی که در آن دولت اظهار می‌دارد که اصول دموکراتیک از جمله بیان حقیقت برای مردم باید در برابر مقاصد سیاست‌های دولتی سر تسلیم فرود آورند. خطر دوم و محتمل‌تر این است که منحرف‌سازی اطلاعاتی مردم خارج از کشور به‌طور غیرعمدی به سمت مردم داخل کشور کشیده شود؛ بدین‌معنی که گمراه کردن خارجی‌ها بدون گمراه کردن شهروندان کشور میسر نیست.

فناوری اشاعه اطلاعات گمراه‌کننده و دست‌کاری ادراکات دشمن می‌تواند به‌آسانی در داخل کشور مورد استفاده قرار گیرد. جالب آنجاست که بسیاری از تسلیحات نبرد اطلاعات را می‌توان علیه مردم داخل کشور به‌کار برد.[2]

۱ـ۶. جنگ سایبر[3]

تعریف

جنگ سایبر[4] همچنین جنگ سایبرنتیک[5] به‌صورت استفاده از کامپیوتر و اینترنت برای

---

1. Ibid
2. Carl Von Clausewitz, **On War,** Michael Howard and Peter Paret, eds. and trans, Princeton; Guildford: Princeton University Press, 1976, book 6, pp. 327-376.
3. Jonathan V. Post, "Cybernetic War," **Omni**, May 1979, PP. 44-104.
4. Cyber warfare
5. Cybernetic

جنگیدن در فضای سایبر تعریف شده است.[1]

انواع حمله

چندین نوع شیوه حمله در این جنگ وجود دارد که در طیفی از کم‌شدت تا شدید دسته‌بندی شده‌اند:

- **خرابکاری اینترنتی**[2]: حملاتی جهت تغییر محتوا و مشکل صفحات وب یا اخلال در سرویس‌دهی[3] که آسیب چندانی را وارد نمی‌سازند.
- **گردآوری داده‌ها**: دسترسی به اطلاعات طبقه‌بندی‌شده که امکان جاسوسی از نقاط مختلف جهان را فراهم می‌کند.
- **حملات گسترده اخلال در سرویس‌دهی**[4]: در این نوع حمله شمار زیادی از کامپیوترها در یک کشور مبادرت به ایجاد اخلال در سرویس‌دهی سیستم‌های کشورهای دیگر می‌کنند.
- **اخلال در تجهیزات**[5]: فعالیت‌های نظامی که در آنها از کامپیوتر و ماهواره برای هماهنگی استفاده می‌شود، در خطر این نوع حمله قرار دارند؛ زیرا مهاجمان می‌توانند فرمان‌ها و ارتباطات را رهگیری کرده، یا تغییر دهند.
- **حمله به زیرساختارهای حیاتی**: نیروگاه‌های برق، تأسیسات آبرسانی و سوخت‌رسانی، ارتباطات و حمل‌ونقل در برابر این نوع حمله با آسیب‌پذیری زیادی مواجه هستند.

تهدید قریب‌الوقوع

هم‌اکنون «جنگ سرد سایبر»[6] تهدیدی بزرگ برای کامپیوترهای جهان به‌شمار می‌رود.

---

1. DOD-Cyberspace.
2. Web Vandalism
3. Denial-of-Service Attacks
4. Distributed Denial-of-Service Attacks
5. Equipment Disruption
6. Cyber Cold War

مک‌آفی، از کمپانی‌های ارائه‌دهنده امنیت اینترنتی، در گزارش سال ۲۰۰۷ خود عنوان کرده بود که به‌طور تقریبی ۱۲۰ کشور درحال توسعه شیوه‌هایی جهت استفاده از اینترنت به‌عنوان یک سلاح هستند که اهداف آنها نیز بازارهای مالی، سیستم‌های کامپیوتری دولت‌ها و تأسیسات حیاتی آنهاست.

در این فعالیت‌ها که یادآور «جنگ سرد» است، آژانس‌های اطلاعاتی به‌طور مرتب شبکه‌ها را برای شناسایی نقاط ضعف آنها کنترل می‌کنند. این تکنیک‌ها برای شناخت نقاط ضعف در اینترنت و شبکه‌های جهانی هرساله رشد بیشتری داشته، پیچیده‌تر می‌شوند.[1]

جف گرین[2]، معاون رئیس آزمایشگاه‌های پیشگیری مک‌آفی[3] عنوان می‌دارد که تبهکاری سایبر[4] هم‌اکنون به موضوعی جهانی تبدیل شده است؛ به‌گونه‌ای‌که نه‌تنها تهدیدی برای صنایع و اشخاص، بلکه تهدید فزاینده‌ای برای امنیت ملی کشورها محسوب می‌شود. به پیش‌بینی وی، این نوع حملات در آینده پیچیده‌تر نیز خواهد شد. گرین می‌گوید «حملات سایبر از کنجکاوی‌های ابتدایی به عملیات‌هایی با منبع مالی، سازماندهی خوب و مقاصد جاسوسی سیاسی، نظامی، اقتصادی و فنی تبدیل شده‌اند.»[5]

گزارش منتشرشده از سوی مک‌آفی نیز می‌گوید که چین در رأس جنگ سایبر قرار دارد، به‌طوری‌که متهم به انجام حملات سایبر ضدسیستم‌های کامپیوتری هندوستان، آلمان و ایالات متحده شده است؛ اما خود این کشور با تکذیب چنین مطلبی ادعا می‌کند که از دانش لازم برای انجام این حملات برخوردار نبوده و از آنجایی‌که دارای بیشترین کامپیوترها در جهان است، توان کنترل همگی آنها را ندارد.[6]

در آوریل سال ۲۰۰۷ نیز کشور استونی ازسوی روسیه مورد حملات سایبر قرار گرفت.

---

1. Griffiths, Peter. "World faces cyber cold war threat", **Reuters,** Retrieved on 2007-11-30.
2. Jeff Green
3. McAfee Avert Labs
4. Cybercrime
5. "Cyber Crime: A 24/7 Global Battle", **Mcafee**, Retrieved on 2007-11-30.
6. "China 'has. 75M zombie computers' in U.S.". Retrieved on 2007-11-30.

این حملات تنها بخشی از حملات گسترده روسیه محسوب می‌شد[1] که این امر نشان می‌دهد «جنگ سرد سایبر» درحال تبدیل شدن به «تهدید قریب‌الوقوع» بین‌المللی است.[2]

حملات معروف

- ایالات متحده مورد حملات کشورهای چین و روسیه بوده است.[3]
- در ماه مه سال ۲۰۰۷ گزارش شد که پارلمان، وزارتخانه‌ها، بانک‌ها و رسانه‌های کشور استونی ازسوی روسیه مورد حمله قرار گرفته‌اند.[4]
- در نخستین هفته از سال ۲۰۰۷ پنتاگون و برخی از کامپیوترهای فرانسوی، آلمانی و انگلیسی مورد حمله هکرهای چینی قرار گرفتند. دولت چین هرگونه دست داشتن دولت در این حملات را رد کرد.
- قرقیزستان نیز در زمان برگزاری انتخابات در این کشور، مورد حمله هکرهای استونی قرار گرفت.[5]

۲. ابزارهای جنگ اطلاعات

ابزارهای جنگ اطلاعاتی نیز همچون مفهوم جنگ اطلاعات گستره وسیع و متنوعی را تشکیل می‌دهند.

از ادوات اولیه استتار تا سلاح‌های مدرن را می‌توان دراین حیطه نام برد؛ اما در اینجا ما به توضیح ابزارهایی که مختص جنگ اطلاعات در عصر جدید هستند خواهیم پرداخت. تسلیحات اطلاعاتی به‌طور گسترده در سه گروه عمده طبقه‌بندی می‌شوند:

1. "Cyberattack in Estonia-what it really means". Retrieved on 2007-11-30.
2. "Exposed Cyber Attacks Could Be the Tip of the Iceberg". Retrieved on 2007-11-30.
3. Jim Wolf, "U.S. Air Force prepares to fight in cyberspace", **Reuters,** Nov. 3, 2006.
4. Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia", The Guardian, May 17, 2007.
5. Website of Kyrgyz Central Election Commission hacked by Estonian hackers, Regnum, 14, Dec. 2007</ref.

۲ـ۱. فرستنده‌های فرکانس رادیویی

نسل جدید این گروه سلاح HERF نامیده می‌شود که به‌معنای فرکانس رادیویی پرانرژی است؛ مخفف زیبایی که حتی گفتنش هم لذت‌بخش است. تاریخچه سلاح‌های مذکور را آغاز دهه ۱۹۷۰ توصیف کرده‌اند.

سلاح HERF وسیله‌ای است که انرژی رادیویی پرقدرت را به هدفی الکترونیک هدایت می‌کند. مدارهای الکترونیک نسبت به تحمل بار اضافی آسیب‌پذیرند. این سلاح به‌آسانی بار اضافی را به مدارهای خاصی وارد می‌نماید تا قطعات مشخصی را که تجهیزات بدان مدارها وابسته هستند ازکار بیندازد. همچنین می‌تواند طوری طراحی شود که درجات مختلفی از خسارت را از خاموش شدن آسان سیستم گرفته تا نابودی فیزیکی تجهیزات ایجاد، و ممکن است با معطوف شدن بر یک کامپیوتر، عملکرد آن را به‌طور موقت یا دائم متوقف نماید.

این فرستنده‌ها اگرچه در نیمه دهه نود، در برد و ظرفیت توان تخریبی محدودیت داشتند، اکنون دارای توانمندی فراوان و به‌راحتی قابل دسترس هستند؛ ازاین‌رو لازم است که این سلاح‌ها جدی گرفته شوند. سلاح‌های HERF ضرورتی فوق‌العاده برای موجودیت نظامی تهاجمی یک دولت بوده، درصورت مالکیت آن توسط دشمن نیز تهدید شاخصی را به نمایش می‌گذارند.[۱]

این سلاح به متخاصمان اجازه می‌دهد که سناریوی حذف کارکرد گستره وسیعی از اهداف را خلق نمایند. ساختن سلاح HERF به‌طرز شگفت‌آوری آسان است. این تسلیحات، بسته به اندازه منبع نیروی مورد استفاده و برد یا دقت عمل مطلوب می‌توانند در اشکال و فرم‌های متفاوتی طراحی شوند. سلاح HERF جریانی از سیگنال‌های رادیویی پرانرژی را به هدفی از پیش تعیین‌شده هدایت می‌نماید.

«مدارهای الکترونیکی بیش از آنچه که اکثر مردم تشخیص می‌دهند به تحمیل بار اضافی[۲]

---

1. C.J. Westwood, **"Military Information Operations in a Conventional Warfare Environment"**, Air Power Studies Centre, APSC, Paper, No. 47, 1997, p.15.
2. Overload

آسیب پذیرند. از این ضعف توسط سلاح HERF بهره‌برداری می‌شود؛ این سلاح، چیزی بیش از یک فرستنده رادیویی نیست و به‌طور ذهنی، شبیه فرستنده‌های واقعاً بلندی است که برفرازشان چراغ‌های قرمزی خاموش و روشن می‌شوند تا از برخورد هواپیماها با آنها جلوگیری گردد. رادیوی پرتابل CB یا تلفن "cellular" نیز نوعی فرستنده رادیویی هستند که با اهداف مختلف و در سطوح قدرت متفاوت کار می‌کنند.

سلاح HERF انرژی کافی به سمت هدف خود شلیک می‌کند تا حداقل به‌طور موقت آن را ازکار بیندازد. این سلاح می‌تواند رایانه یا کل شبکه‌ای را ازکار متوقف کند یا سوئیچ تلفنی را درون مداری الکترونیکی ارسال نماید. مدار درون رایانه و تجهیزات مدرن برای سیگنال‌ها، در سطوح پایین[1] طراحی شده است. صفر و یک‌های خیلی ظریفی درون حدهای نرمال کارکرد دارند. سلاح HERF برای تحمیل بار اضافی به این مدار الکترونیکی طراحی شده است؛ به‌گونه‌ای‌که سیستم اطلاعات مورد حمله، لااقل به‌طور موقت تبدیل به سلسله بی‌معنایی از «بایت‌های» پاره‌پاره می‌گردد».[2]

خسارتی را که سلاح HERF می‌تواند به گستره متنوعی از اهداف گزینش‌شده به‌شکل خلاقانه وارد نماید، آشکار است. سیستم‌های اطلاعاتی نه‌تنها در چنین وضعیت خلق‌شده‌ای ازکار می‌افتند، بلکه به‌طرز فوق‌العاده‌ای، تشخیص هویت عامل این ازکار افتادن مشکل است.

این اسلحه، سلاح بسیار قدرتمندی در زرادخانه جنگجویان اطلاعاتی است که بنابر احتیاجات موردنظر در قطعات و اندازه‌های گوناگون عرضه می‌شود. در سطح بسیار پایه نیز این سلاح، سیگنال رادیویی بسیار نیرومندی را به‌سوی یک نوع هدف الکترونیکی شلیک می‌کند و آن را غیرقابل استفاده و عاطل‌وباطل می‌سازد.

اسلحه HERF برای جنگجویان اطلاعاتی کارآمد عمل خواهد کرد، منوط‌برآنکه چند معیار

---

1. low level
2. Winn Schwartau , **Information Warfare : Chaos on the Electronic Superhighway**, New York : Thunder's Mouth, 1994, p. 179.

رعایت شود: اول آنکه، این اسلحه باید تاجایی‌که می‌تواند انرژی منتشر سازد و هرچقدر انرژی بیشتری از خود ساطع کند، به همان نسبت می‌تواند صدمات بیشتری وارد کند؛ دوم آنکه، باید نسبت به مکانی که گلوله‌های مغناطیسی‌اش را شلیک می‌کند، از قدری کنترل و جهت‌گیری برخوردار باشد. بعضی از انواع این اسلحه‌ها شبیه تفنگ ساچمه‌ای هستند که تشعشعشان در همه‌جهت پخش می‌شود، بعضی از انواع آنها نیز شبیه به تفنگ‌های دقیق، فوق‌العاده متمرکز عمل می‌کنند. اسلحه HERF می‌تواند سلاح خیلی ساده یا فوق‌العاده پیچیده‌ای باشد و در کامیونی مملو از وسایل و ابزار جابجا گردد.

اما همه این سلاح‌ها دارای قطعات ساده مشابهی هستند که عبارتند از: یک منبع انرژی، یک نوع روش ذخیره انرژی تا زمانی‌که تخلیه شود و یک ابزار خروجی یا آنتن. سایر چیزها هم موجود هستند.

می‌توان با سلاح‌های الکترومغناطیسی به اهدافی اینچنین دست یافت:

- محرومیت از حمل‌ونقل پرسنل؛[1]
- ترساندن مخالفان؛[2]
- اختلال در ارتباطات؛[3]
- تخریب قابلیت ADP؛[4]
- اختلال در سرویس‌های حمل‌ونقل؛[5]
- خرابکاری؛[6]
- تروریسم/ ضدتروریسم؛[7]
- دفاع زمینی/ هوایی؛[8]

1. Personnel and Transportation Interdiction
2. Harassment of Opposition
3. Communications Disruption
4. Destruction of ADP Capabiliy
5. Interruption of Transportation Services
6. Sabotage
7. Terrorism/Anti-Terrorism
8. Air/Land Defense

- تهاجم نظامی؛[1]
- فعال‌سازی یا برانگیختگی حکم دشمن؛[2]
- تداخل ارتباطی؛[3]
- تخریب قطعات الکترونیکی.[4]

اسلحه HERF چالش واقعی را برای بخش تجاری، به‌ویژه اگر مورد استفاده تروریست‌ها قرار گیرد، به نمایش می‌گذارد.

۲ـ۲. پرتابگرهای پالس الکترومگنتیک

اگر اسلحه HERF بسیار کوچک‌تر از آنی است که بتواند زیان و خسارت موردنظر جنگجویان اطلاعاتی را وارد سازد، شاید فرستنده پالس الکترومغناطیس یا بمب EMP برای این هدف مناسب‌تر باشد. بمب EMP در اصل مانند اسلحه HERF و البته هزار برابر از آن قدرتمندتر است.

این سلاح به‌منزله اسلحه عظیم دیگری برای تکامل جنگ نوین توصیف می‌شود. این پدیده که در آغاز به‌عنوان اثر جانبی آزمایش‌های هسته‌ای کشف شد، اکنون به مولدهای غیرهسته‌ای گسترش یافته است. این مولدها می‌توانند یک EMP ایجاد نمایند که سیستم‌های الکترونیکی بی‌حفاظ را ناتوان سازد. مولد پیشرفته‌ای را با ظرفیت یک گیگاوات می‌توان طوری به‌کار گرفت که بسته به روش به‌کارگیری خط نشانه، EMP را به‌وجود آورد که به اکثر دستگاه‌های الکترونیکی در شعاعی قابل اندازه‌گیری در فواصلی تا صدها متر ضربه وارد نماید.[5]

بمب‌های مبدل (ترانسفورماتور) پالس الکترومگنتیک، تحت اصول مشابهی با تسلیحات HERF عمل می‌کنند؛ اما هزاران مرتبه قوی‌تر هستند و خساراتی را که به‌بار می‌آورند دائمی‌است؛ زیرا دولت‌ها از زمان اختراع بمب اتم با تهدید پالس الکترومگنتیک سروکار داشته‌اند.

---

1. Millitary Offensive
2. Enemy Ordinance Activation
3. Communications Interference
4. Electronic Component Destruction
5. Westwood , Ibid.

سخت‌افزارهای ذیل برخی از مواردی هستند که بیشترین آسیب‌پذیری را در مقابل EMP دارند:

رایانه‌ها، تجهیزات برق رایانه، تجهیزات برق ترانزیستوری، اجزای نیمه‌هادی خطوط کابلی طولانی، سیستم‌های اخطاردهی[1]، سیستم‌های intercom، وسائل تلفنی، سیستم‌های کنترل فرایند ترانزیستوری، گیرنده و فرستنده‌های ترانزیستوری، سیستم‌های کنترل نیروی برق، خطوط ارتباطاتی، ماکروویوهای پرقدرت و سیستم پردازش داده‌های کامپیوتری.[2]

پیش از این محدودیت چنین تسلیحاتی، تولید نیرو و توانمندی و ظرفیت ذخیره‌سازی آنها قلمداد می‌شد.

سیگنال یا پالس الکترومغناطیسی که با سرعت نور از یک بمب EMP پرتاب می‌شود، از چنان قدرت خارق‌العاده‌ای برخوردار است که هر کامپیوتری در مسیرش قرار داشته باشد، احتمالاً برای همیشه به شیئی بی‌خاصیت مبدل خواهد شد.

ارگان‌های داخلی و تراشه‌های آن طوری ذوب خواهند شد که قابل تعمیر نخواهند بود؛ اما نکات بیشتری هم وجود دارد. با یک نوع سیگنال الکترومغناطیسی با آن قدرت، تمامی دیسک‌های فلاپی، دیسک‌های سخت، نوارها و پشتیبان نواری پاک خواهند شد. همه اطلاعات و داده‌ها برای همیشه ازبین خواهند رفت. بمب EMP نوعی سلاح بسیار غافلگیرکننده در دستان جنگجوی اطلاعاتی است و در موارد متعدد، این سلاح‌های تکنیکی پیشرفته توسط پنتاگون آفریده شده‌اند.

ارتش آمریکا تقریباً نزدیک به دو دهه به آنچه سلاح‌های غیرمرگبار[3] نامیده شده‌اند، علاقه‌مند بوده است. منظور از سلاح‌های غیرمرگبار، سلاح‌هایی هستند که هدف عمده‌شان کشتن دشمنان نیست؛ بلکه می‌خواهند آنان را چنان عاجز و ناتوان سازند تا نتوانند جنگی را آغاز کنند.

---

1. alarm
2. Federal Emergency Management Agency , "EMP Threat and Protective Measure", **Report for Public Distribution,** Apr. 1980, p. 11
3. Nonlethal Weapens

«این نوع سلاح‌ها بدون آنکه انسان‌ها را بکشند، می‌توانند تلفن‌ها، رادارها، کامپیوترها و ارتباطات و ابزاروسایل مورد هدف را مختل سازند».

ازقرار معلوم ایالات متحده در خلال جنگ خلیج‌فارس از این قبیل سلاح‌های اطلاعاتی[1] استفاده کرد. در ۱۵ آوریل سال ۱۹۹۲ میلادی، در نشریه دیفنس ویک[2] عنوان شد که «نیروی دریایی آمریکا در ساعات آغازین جنگ خلیج‌فارس از نوعی کلاهک الکترومغناطیسی غیراتمی استفاده کرد تا ازاین‌طریق سیستم‌های الکترونیکی عراقی، ازجمله سلاح‌های دفاع هوایی و مراکز فرماندهی و کنترل، صنایع نظامی و صنعتی آن کشور را مختل و نابود سازد». این سلاح‌های آزمایشی از قرار معلوم بر روی تعداد اندکی از موشک‌های کروز تام هاگ نصب شده بودند.

آزمایشگاه‌های ماکسول،[3] پیمان‌کاری از وزارت دفاع و متخصص در سلاح‌های پرانرژی است که در سال ۱۹۹۲ مقاله‌ای را تحت عنوان «به‌کارگیری منابع مایکروویوهای پرقدرت در خرابکاری الکترونیکی و تروریسم» منتشر کرد. نویسندگان مقاله تاریخچه سلاح‌های سبک HERF در آغاز سال‌های ۱۹۷۰ را توصیف کردند.

منابع میکروویوهای پرقدرت به‌مدت چند سال به‌عنوان سلاح‌های بالقوه برای انواع خرابکاری، تروریسم، کاربردهای نبردی و ضدامنیتی مورد بررسی و تحقیق قرار گرفته‌اند. البته در سال‌های اخیر، آگاهی فزاینده درباره اچ.پی.ام (نوعی HERF) به‌مثابه ابزاری برای خرابکاری تجاری و تروریسم مدنی وجود داشته است.

چندین مقاله مشابه دراین‌خصوص به توصیف تکنیک‌هایی می‌پردازند که این قبیل سلاح‌های الکترونیکی کاربردی می‌نماید. زبان مورد مصرف پیمان‌کاران وزارت دفاع فوق‌العاده تکنیکی است که به توصیف روش‌های انفجار از قبیل Slugtuning، Magnetrons، Vircqtors و لوله‌های نوسانگر از لحاظ مغناطیسی عایق‌سازی شده می‌پردازد. بخش ترسناک

---

1. Information Weapons
2. Defense Week
3. Maxwell Laboratories

آن گسیختگی در نگارش این مقالات است.

در مورد همه حملات شهری، به‌استثنای تروریسم‌های پیشرفته توقع می‌رود که از منابع الکترونیکی (نیرو) استفاده خواهد شد. برای حملات کوتاه‌برد و جهت‌دار از سطوح «زیرمگاوات»[1] استفاده خواهد شد. برای بردهای طولانی یا تشعشع چندجهتی از نیروهای بیشتر و هنوز دست‌یافتنی‌تر استفاده خواهد شد. البته باید گفت که «به‌دلیل محدودیت‌هایی که در زمینه طبقه‌بندی وجود دارد، این مطالعه در خارج از جامعه نظامی و پیمان‌کارانش شناخته شده نیست. اما مهار تکنولوژی پیشرفته فوق‌العاده دشوار است؛ به‌این‌دلیل که سایر کشورها به موازات مطالعات محرمانه آمریکا در مورد سلاح‌های HERF پیش می‌روند. در موارد متعدد اگر ارتش آن را داشته باشد به‌سرعت به دست افراد تروریست می‌افتد. ای.آر.ون کیودن، کارشناس انرژی‌های سطح بالا در سندی مقدماتی عنوان می‌کند که «وقتی درباره تروریسم و خرابکاری بحث می‌کنیم، دشمنان کمتر رغبت به آن دارند که سلاح‌هایشان را در دسترس ملت‌های تروریست یا ایالات‌متحده قرار دهند».

سلاح‌های HERF و بمب‌های EMP به‌عنوان سلاح نهایی، اهداف جنگجوی اطلاعاتی را برآورده می‌کنند. بازسازی سیستم‌های کامپیوتری و مرمت پایگاه‌های داده نرم‌افزاری از روی سوابق کاغذی، بدون تردید ماه‌ها به‌طول خواهد انجامید.

۳ـ۳. سایر تسلیحات اطلاعاتی

تسلیحات متعدد دیگری نیز وجود دارد که درحال گسترش هستند. این تسلیحات در قالب EMP و HERF نمی‌گنجند. برخی از آنها قبلاً در نیروهای متنوع نظامی‌مورد استفاده قرار گرفته‌اند و برخی نیز هنوز در مرحله طراحی هستند.

تسلیحات ذیل ازجمله این گروه سلاح‌ها و قابل دسترسی هستند:

---

1. Submegawatt

۲ـ۳ـ۱. *لیزرهای کم‌انرژی*

این لیزرها می‌توانند برای آسیب زدن به سیستم‌های نوری حسگرها، شامل: دستگاه‌های جمع‌آوری داده‌ها مورد استفاده قرار گیرند؛ ازاین‌رو به سیستم‌های اطلاعاتی در سطح جمع‌آوری داده‌ها حمله می‌کنند. لیزرهای کم‌انرژی قبلاً روی تفنگ‌ها و خودروهای زرهی نصب شده و در طی جنگ خلیج فارس نیز به‌کار گرفته شده‌اند.[1]

۲ـ۳ـ۲. *بمب الیاف کربنی*[2]

نسخه‌های اولیه بمب الیاف کربنی، نیروگاه‌های بغداد را طی جنگ خلیج فارس ازکار انداخت. موشک‌های کروزی که با حلقه‌های کربنی فوق‌العاده باریکی خرج‌گذاری شدند، فقط برفراز دستگاه‌های الکترونیکی منفجر می‌شدند و رشته‌های گسترده‌شده بر مدار بیرونی فروآمده، دستگاه‌ها را از مدار خارج می‌کنند.

ایالات‌متحده آمریکا ادعا می‌کند که زمانی این فناوری را به‌کار می‌برد که بخواهد خسارات بلندمدت به زیر ساخت‌های مدنی را به حداقل برساند. اگر این رشته‌ها زدوده شوند، دستگاه‌ها دوباره به‌کار خواهند افتاد و این کار تنها چند روز به‌طول می‌انجامد. همچنین این بمب‌ها صدمه به کارخانه‌های برق را به حداقل می‌رسانند.

در سال ۱۹۹۵ Aviation Week and Space Technology گزارش داد که پنتاگون این سلاح را بهبود بخشیده است. این بمب فیبرهای الیاف کربنی باریکی را با ابری متراکم و با حرکت آرام از روی هدف عبور می‌دهد. فیبرها به درون کانال‌های تهویه ساختمان‌ها و وسائل نقلیه جاری شده و هر وسیله الکترونیکی را از داخل قطع مدار می‌کند. تنها خطر شناخته شده این بمب‌ها برای انسان این است که فیبرهای مذکور می‌توانند بیماری‌های پوستی شدیدی ایجاد نمایند. این بمب‌ها در جنگ ناتو علیه یوگسلاوی و جنگ نفت علیه عراق نیز به‌کار گرفته شد.[3]

---

1. Winn Schwartau, op.cit. , p. 180 2. Carbon Filament Bomb
3. A Bomb that drops Spools of Wire, Ibid.

۲ـ۴. برنامه‌های رایانه‌ای

نفوذگران رایانه‌ای از برخی تکنیک‌های متنوع زیر جهت نفوذ در سیستم‌های اطلاعاتی استفاده می‌کنند:

۲ـ۴ـ۱. کرم‌ها

«کرم‌ها» برنامه‌ای مستقل است که به‌طور شعله‌ور خود را تکثیر می‌کند و از کامپیوتری به کامپیوتر دیگر و اغلب روی شبکه‌ها می‌رود و برخلاف ویروس‌ها برنامه‌های دیگر را تغییر نمی‌دهد.

پیامدهای مخرب این جنگ‌افزار در دو زمینه قابل بررسی است که:

یکی نابودی منابع موجود اطلاعاتی در شبکه و دیگری تغییر شکل و انتشار در شبکه است.

۲ـ۴ـ۲. تروجان (اسب تروا)

تروجان‌ها برنامه‌هایی هستند که در داخل سایر برنامه‌ها پنهان می‌شوند و برنامه خود را به اجرا درمی‌آورند. اسب تروا می‌تواند خود را استتار کند و حتی در برنامه‌های شبکه مانند SATAN قرار بگیرد.

۲ـ۴ـ۳. بمب منطقی

بمب منطقی نوعی اسبترواست که برای آزاد کردن ویروس‌ها یا سیستم‌های تهاجمی دیگر مورد استفاده قرار می‌گیرد و می‌تواند به‌صورت برنامه‌ای مستقل که توسط برنامه‌نویس و طراح در سیستم جاسازی می‌شود عمل کند. نظربه‌اینکه تعداد زیادی نرم‌افزار از آمریکا صادر می‌شود، پیشنهاد شده است که در نرم‌افزارهای صادراتی، اسب تروا نصب شود. این عامل مخفی می‌تواند درشرایطی‌که آن کشور علیه آمریکا وارد جنگ شده است، از راه دور فعال شده و آثار مخرب آن می‌تواند شامل «فرمت کردن» دیسکت سخت یا ارسال اسناد به سازمان سیا باشد.

۲ـ۴ـ۴. میکروب‌ها

میکروب‌ها می‌توانند تخریب‌های شدیدی در سیستم‌ها به وجود آورند و برخلاف ویروس‌ها بر روی سخت‌افزارها (و نه نرم‌افزارها) مؤثر واقع شوند. با توجه به اینکه میکروب‌هایی وجود دارند که نفت می‌خورند، این پرسش مطرح می‌شود که آیا می‌توان آنها را برای خوردن ماده سیلیسیوم پرورش داد؟ درصورت عملی بودن، می‌توان پیش‌بینی کرد که بتوان کلیه مدارهای مجتمع را تخریب کرد.

۲ـ۴ـ۵. ویروس‌ها

شایع‌ترین ابزار عملیات رایانه‌ای، استفاده از ویروس است. ویروس‌ها برنامه‌هایی هستند که می‌توانند خود را به برنامه‌های بزرگ‌تر تکثیر کنند. برنامه‌های ویروس وقتی فعال می‌شوند که برنامه میزبان شروع به فعالیت کند؛ به‌دنبال آن، ویروس خود را تکثیر و برنامه‌های دیگر را آلوده می‌کند. ویروس‌ها در هر محیط کامپیوتری وارد می‌شوند و تعجب‌آور نیست که به‌مثابه جنگ‌افزار اطلاعاتی مورد استفاده قرار بگیرند. وقتی یک هکر، ویروس را به داخل شبکه‌های کامپیوتری فرستاده باشد، شبکه هدف ازکار می‌افتد یا لااقل نارسایی‌های وسیعی در آن ایجاد می‌شود.[1]

۲ـ۴ـ۶. تخریب تراشه[2]

اکثر مردم به آسیب‌پذیری نرم‌افزارها در قبال نفوذهای خصمانه آگاهی دارند، مانند حملات ویروس؛ اما تعداد کمی از آنها از خطر اجزای اساسی نرم‌افزارهای سیستم اطلاعاتی آگاه هستند. تخریب تراشه واژه‌ای است که به وقایع غیرمنتظره اشاره دارد که می‌توانند درون تراشه‌های کامپیوتری طراحی شوند. امروزه تراشه‌ها حاوی میلیون‌ها مدار یکپارچه هستند که

---

۱. مرادعلی صدوقی، **تکنولوژی اطلاعاتی و حاکمیت ملی**، تهران: وزارت امورخارجه، مرکز چاپ و انتشارات، ۱۳۸۰.

2. Chipping

می‌توانند بـه آسـانی توسـط تولیدکننـدگان بـه‌گونـه‌ای پیکربنـدی شـوند تـا بتواننـد حـوادث غیرمترقبه‌ای را در زمانی خاص یا هنگام وقوع اوضاع ویژه آغاز نمایند. بدین‌ترتیـب مـی‌تـوان توضیح داد که چرا برخی از کالاهای الکترونیک پس از مدت کوتاهی از انقضای گارانتی ازکار می‌افتند. تقریباً هیچ راهی برای کشف اینکه تراشه‌ای در درون خود حاوی قطعـه‌ای اسـت کـه تجهیزات را منحرف می‌نماید، وجود ندارد.

روش پیشنهادی برای کمتر ساختن مخاطرات تخریب تراشه، تولید تمامی‌تراشـه‌هـای مهـم در داخل کشور است؛ مانند تراشه‌هایی که در سیـستم کنتـرل هـوایی و ناوگـان هـوایی مـورد استفاده قرار می‌گیرند؛ اما از نظر اقتصادی، اغلب این مسئله امکان پذیر نیست. اکثر تراشه‌هایی که امروزه درون تجهیزات با تکنولوژی بالا استفاده می‌شوند، در کـشورهایی کـه حقـوق‌هـای کارگری پایین است، تولید می‌گردند.

تخریب تراشه روشی آسان جهت توسعه برتری نظامی متعارف توسط آن‌دسته کـشورهایی است که به‌گونه‌ای قاعده‌مند و منظم تجهیزات نظامی صادر می‌کنند و درصورت وقوع هرنـوع مخاصمه‌ای با دریافت‌کنندگان تجهیزات تراشه‌شده ممکن است این تجهیزات بـدون اجبـار در به‌کارگیری متعارف زور ازکار بیفتند. دراینجا اقتصاد به اندازه نیروی نظـامی اهمیـت مـی‌یابـد. وجه‌های حقوقی و اخلاقی این قضیه، موضوعاتی مجزا هستند.[۱]

دراین‌زمینه می‌توان از اقدامات پیشگیرانه چین یاد کرد که فرض را بر این گذاشته از قبل مورد حمله الکترونیکـی - سـایبرنتیکی ایـالات متحـده آمریکـا واقـع شـده اسـت.«تمـامی‌قطعـات سخت‌افزار و نرم‌افزار کامپیوتر که از آمریکا یـا متحـدان آن وارد مـی‌شـود، موقـع رسـیدن بـه مرزهای چین مورد بازرسی و بازبینی دقیق قرار می‌گیرد و تکنسین‌های چینی هر قطعه‌ای را که متخصصان غربی به روی تجهیزات خـود نـصب کـرده‌انـد کنتـرل مـی‌کننـد. چنـین کنتـرل و محدودسازی در روسیه نیز اجرا می‌شود».[۲]

---

1. C. J. Westwood, op.cit., p. 14.

۲. جیمز آدامز، «دفاع مجازی»، ترجمه: حسین سلیمی، **فصلنامه سیاست خارجی**، سال پانزدهم، شماره ۳، پاییز ۱۳۸۰.

فصل پنجم
تکنولوژی‌های حفاظت در نبرد اطلاعات

- روش‌های حفظ و نگهداری اطلاعات
- قفل و کلید
- روش‌های تایید اعتبار
- امنیت اطلاعات و تضمین اطلاعاتی

۱. روش‌های حفظ و نگهداری اطلاعات

یکی از راه‌های حفاظت از منابع اطلاعاتی، پنهان کردن آنها از چشم‌ها یا در پشت قفل فیزیکی یا دیجیتالی است. هفت شیوه برای حفاظت از منابع اطلاعاتی وجود دارد که عبارتند از:

- قفل‌ها و کلیدهای فیزیکی؛
- رمزی‌سازی؛
- سرّی‌نگاری[1]؛
- گمنام‌سازی[2]؛
- بهداشتی کردن[3]؛
- دفع آشغال[4]؛
- سپرسازی.

۱ـ۱. قفل و کلید

از قفل و کلید می‌توان برای حفاظت از انواع واسطه‌های فیزیکی ازجمله: محیط فیزیکی، کاغذها، دیسکت‌ها، نوارها، سیستم‌های رایانه‌ای و مخابراتی محلی استفاده کرد. قفل را می‌توان بر روی درهای ساختمان‌ها و ادارات، درهای خروجی، گاوصندوق‌ها، میزها، کشوهای بایگانی

---

1. Steganography
2. Unonymity
3. Sanitization
4. Trash Disposal

و هر ظرف فیزیکی قرار داد.

قفل هم ابزار کنترل دسترسی انفعالی و هم سازوکاری برای پنهان کردن محتوای شیء قفل شده است. فناوری قفل نیز شامل: کلید فیزیکی، قفل رمزدار و دسته‌کلید الکترونیکی است.

قفل‌ها محدودیت‌هایی هم دارند؛ بیشتر آنها را می‌توان شکست یا از آنها عبور کرد (اغلب توسط قفل‌سازهای معمولی). کلیدها ممکن است در جایی گذاشته شوند که افراد غیرمجاز به آنها دسترسی پیدا کنند یا به کسانی که نباید کلید داشته باشند داده شوند. کارمندان ممکن است هنگام ترک اتاق کار خود، اتاق، میز و کابینت بایگانی را قفل نکنند یا به‌منظور نشان دادن ادب، ممکن است در را به روی کسانی که اجازه دسترسی ندارند باز بگذارند. وقتی کارمندی اخراج یا بازنشسته می‌شود، ممکن است سازمان، کلیدها را نگیرد یا قفل و دسته‌کلید را عوض نکند. یک کارمند سابق ناراضی می‌تواند برگردد و منابع اطلاعات را بدزدد یا در آنها خرابکاری کند.

۱ـ۲. رمزی‌سازی

رمزی‌سازی برای اطلاعات، حکم قفل برای اطلاعات چاپی را دارد. اطلاعات به‌وسیله درهم‌سازی به‌نحوی که فقط با یک کلید محرمانه از حالت درهم خارج شود، مورد حفاظت قرار می‌گیرد. پیام درهم ریخته‌شده که «متن سرّی»[1] نامیده می‌شود، به‌طورکلی برای کسی که کلید را نداشته باشد ناخوانا است. فرایند ایجاد متن سرّی را «سرّی‌سازی»[2] یا «رمزی‌سازی»[3] می‌نامند.

فرایند معکوس، یعنی احیای پیام اصلی ـ که متن ساده نام دارد ـ «آشکارسازی»[4] یا «سرگشایی»[5] نامیده می‌شود. یک روش خاص سرّی‌سازی و آشکارسازی، «سیستم رمزی‌نگاری»[6] یا «سیستم رمزی»[7] نامیده می‌شود. تمام رمزها با دو نوع اصلی دگرگونی شکل،

---

1. Ciphertext
2. Enciphernment
3. Encryption
4. Deciphernment
5. Decryption
6. Cryptographinc System
7. Crypto System

یعنی با «جایگشت»[1] و جانشینی تشکیل می‌شوند. در جایگشت، ترتیب قرار گرفتن کاراکترها یا «بیت‌ها»[2] تغییر می‌کند؛ درحالی‌که در جانشینی، بیت‌ها، کاراکترها یا بلوک‌ها تغییر می‌کنند و بیت‌ها، کاراکترها یا بلوک‌های دیگری جانشین آنها می‌شوند. این دگرگونی‌های شکلی، طوری مرتب می‌شوند که برای رسیدن به نتایج متفاوت می‌توان روش واحدی را با کلیدهای مختلف به‌کار گرفت. برای «سرگشایی» شخص باید هم به روش و هم به کلیدی که رمزی‌سازی با آن انجام شده، آگاهی داشته باشد. درحالی‌که کلیدها محرمانه نگاه داشته می‌شوند، خود روش اغلب علنی است؛ زیرا بسیاری از افراد می‌توانند در آن سهیم باشند و از آن در محصولات نرم‌افزاری و سخت‌افزاری استفاده کنند.

۱ـ۲ـ۱. رمز دیجیتالی: سیستم‌های رمزنگاری امروزی با برنامه‌های رایانه‌ای که دو ورودی (پیام رمزی نشده و کلید) دارند انجام می‌شوند. هر دو ورودی به‌صورت صفرها و یک‌ها هستند.

قدرت یک سیستم رمزی در توانمندی آن در مقاومت در برابر حملات اشخاصی است که به متن سرّی دست می‌یابند. به‌جز یک استثنا، در عالم نظری تمام رمزها با امتحان کردن تمام کلیدهای ممکن، قابل شکستن هستند؛ ولی این بدان معنا نیست که در عمل می‌توان رمزها را شکست. اگر طول کلید به اندازه کافی زیاد باشد، امتحان کردن تمام کلیدها، یک به یک غیرممکن است. در عمل، قدرت یک سیستم باید با خطر و پیامدهای شکسته شدن تناسب داشته باشد. سیستمی که اصلاً شکسته‌شدنی نیست (حتی در تئوری)، سیستم «دسته‌کلید یک‌بار مصرف»[3] است. این سیستم از یک جریان کلید که به‌طور تصادفی ایجاد می‌شود و دسته کلید نیز نامیده می‌شود و طول آن برابر پیام است استفاده می‌کند و از هیچ دسته‌کلیدی بیش از

1. Transposition
2. Bites
3. One-Time Pad

یک‌بار استفاده نمی‌شود. برای تضمین سرّی بودن کامل، دسته‌کلید باید با فرایند واقعاً تصادفی ـ که خود این کار، کار کوچکی نیست ـ به‌وجود آید. درغیراین‌صورت ممکن است از الگوها، قابل استنباط باشد. در بسیاری از محیط‌های کاربردی، به‌علت مشکلات رساندن دسته‌کلید از یک کانال مطمئن به گیرنده، سیستم دسته‌کلید یک‌بار مصرف غیرعملی است. در عوض رمزهای جریان، به‌وسیله استفاده از یک «کلید ایجادکن شبه تصادفی»[1] یک دسته‌کلید یک‌بار مصرف ایجاد می‌کند که ممکن است از امنیت برخوردار باشد یا نباشد. یکی از رایج‌ترین رمزها، «استاندارد سرّی‌سازی داده‌ها»ست.

از استاندارد سرّی‌سازی داده‌ها می‌توان برای سرّی‌سازی یک پیام یا سند طولانی استفاده کرد. این کار «حالت کتاب رمز الکترونیکی»[2] نامیده می‌شود. از استاندارد سرّی‌سازی داده‌ها، می‌توان در سه حالت: پس‌خوراند خروجی[3]؛ پس‌خوراند سرّی و زنجیره‌ای‌سازی بلوک سرّی استفاده کرد.

در پس‌خوراند خروجی، از استاندارد سرّی‌سازی داده‌ها، برای ایجاد یک جریان کلید استفاده می‌شود. این کار با رمزی‌سازی یک بلوک اولیه داده‌ها انجام می‌شود. آن بلوک نیز مجدداً رمزی می‌شود. این جریان آنقدر ادامه می‌یابد که جریان کلید هم‌طولِ متن ساده رمزی‌نشده گردد. گیرنده با تکرار معکوس همان فرایند، با استفاده از کلید و بلوک اولیه، از جریان رمزگشایی می‌کند. پس‌خوراند خروجی، معمولاً با ارتباطات تلفنی سرّی‌شده مورد استفاده قرار می‌گیرد. در زنجیره‌سازی، بلوک سرّی یکایک بلوک‌های ورودی، با بلوک متن ساده ادغام می‌شوند. زنجیره‌سازی بلوک سرّی به‌طور گسترده در فایل‌ها و پیام‌های رایانه‌ای مورد استفاده قرار می‌گیرد. این روش که توسط شرکت IBM ایجاد گردیده، در سال ۱۹۷۷ توسط دولت آمریکا به‌عنوان استاندارد پذیرفته شده است.

---

1. Pseu do Random
2. Electronic Codebook Mode
3. Output Feedback

۱ـ۲ـ۲. رمزشکنی: رمزشکنی فرایند پی بردن به متن ساده یک متن سرّی، بدون دانستن کلید رمز یا احتمالاً بدون دانستن روش سرّی‌سازی است. اگرچه رمزشکنی جزء روش جنگ‌های اطلاعاتی تهاجمی است، به دو دلیل در نبرد اطلاعاتی دفاع‌محور نیز مورد بحث قرار می‌گیرد: نخست، با مقداری زمینه در مورد رمزی‌سازی، درک آن آسان‌تر می‌شود و دوم، در ایجاد رمزهای دارای امنیت نقش حساسی ایفا می‌کند. بدون درک کامل چگونگی حمله به رمزها و بدون آزمایش آنها ازنظر آسیب‌پذیری، طراحی سیستم رمزی مطمئن غیرممکن است. رمزشکنی جزء اصلی رمزی‌سازی است. در رمزشکنی ترکیبی از تجزیه و تحلیل‌ها و آزمایش و خطای ساده دخالت دارند. گام اول، تعیین روش رمزی‌سازی و طول کلید و معمولاً از ۴۰ تا ۱۲۸ بیت است، ولی ممکن است طولانی‌تر نیز باشد. این مطلب اغلب به آسانی ازطریق اطلاعاتی که به متن سرّی پیوست است یا علم به محصولی که برای رمزی‌سازی مورد استفاده قرار گرفته، معلوم می‌شود. وقتی روش رمزی‌سازی و اندازه کلید معلوم شد گام بعدی تعیین کلید است. با پی بردن به کلید، متن سرّی‌شده مورد رمزگشایی قرار گرفته است. اگر برای چند پیام یا طی مدتی طولانی از یک کلید استفاده شده باشد، کار رمزگشایی ساده‌تر است؛ ولی اگر برای هر پیام یا فایل از کلید متفاوتی استفاده شده باشد، تحلیل‌گر رمز (رمزشکن) باید روی یکایک آنها کار کرده، کلید هر یک را پیدا کند.

۱ـ۲ـ۳. ایجاد و توزیع کلیدها: ایجاد یک رمز قوی فقط گام اولی است که به‌سوی امنیت برداشته می‌شود. آنچه به‌همان اندازه چالش‌برانگیز است، مدیریت کلید است که شامل: ایجاد، توزیع، نگاهداری و بازیافت کلیدهای سرّی می‌شود.

برنامه‌هایی که کلیدها را ایجاد می‌کنند درنوع خود از فرایند شبه‌تصادفی که شامل: خواندن اطلاعات حالت سیستم (مثلاً وقت در ساعت) است، استفاده می‌کنند. غیر از حالتی که این مقادیر، غیرقابل پیش‌بینی بوده، تغییرپذیری کافی داشته باشند، دشمن ممکن است قادر شود با مشاهده سیستم، کلید را تعیین کند؛ برای مثال مدت کوتاهی پس از آنکه برنامه‌نویسی

فرانسوی کلید چهل بیتی «نت اسکیپ»[1] را شکست، «یان گلدبرگ» و دانشجوی دیگری از دانشگاه برکلی به نام «دیوید واگنر» دریافتند که کلیدهای نت اسکیپ را صرف‌نظر از اینکه چهل بیتی باشند یا ۱۲۸ بیتی اغلب می‌توان شکست. موضوع این بود که کلیدها از مقادیری ایجاد شده بودند که هرکس با ماشین آشنایی داشته باشد، می‌تواند آن را تعیین کند یا حدس بزند. (در پاره‌ای موارد ظرف ۲۵ ثانیه) وضع طوری بود که انگار کلیدها فقط بیست بیت طول دارند. نت اسکیپ بعداً مشکل را اصلاح کرد.

در بعضی کاربردها، کاربران کلیدهای خاص خود را ایجاد می‌کنند یا در فرایند ایجاد کلید شرکت می‌کنند؛ برای مثال آنها ممکن است کلمه عبوری را که به‌عنوان کلید مورد استفاده قرار می‌گیرد تعیین کنند یا بر صفحه کلید، کاراکترهای تصادفی تایپ کنند که با زمان ساعت و سایر اطلاعات حالت سیستم مورد استفاده قرار می‌گیرد و یک کلید تصادفی ایجاد می‌کند. نقطه‌ضعف‌های کلمات عبور در این چارچوب، همان نقطه‌ضعف‌هایی است که محیط‌های دیگر دارند. وقتی رمزی‌سازی برای محافظت از ارتباطات مورد استفاده قرار می‌گیرد، پاره‌ای روش‌ها مورد نیاز است تا فرستنده و گیرنده بتوانند روی یک کلید سرّی توافق کنند؛ ولی به دلایل روشن، فرستنده نمی‌تواند کلید را به‌طور واضح به دریافت‌کننده بفرستد. اگر کانال مطمئن بود نیازی به رمزی‌سازی نبود، ولی این اغلب عملی نیست؛ زیرا طرفین ممکن است در دو سوی یک قاره یا جهان باشند.

رویکرد دوم این است که کلید را از کانال مطمئن دیگری ارسال کنند؛ مثلا به‌وسیله یک پیک قابل اعتماد.

عیب رویکرد دوم تأخیری است که به‌وجود می‌آید. در کاربردهای بسیاری مانند تجارت الکترونیک، کاربران و برنامه‌هایی که ازطریق آنها اجرا می‌شوند، نیازمند راهی هستند که کلید را به‌سرعت دریافت کنند.

---

1. Netseape

رویکرد سوم استفاده از یک مرکز قابل اعتماد کلید است که با هر فرد، رمز درازمدت مشترکی دارد. این کلیدها باید در خارج از شبکه ایجاد و توزیع شوند. سپس برای مثال، وقتی طرف الف می‌خواهد پیامی را به ب ارسال کند، الف با ذکر نام خود و ب، از مرکز کلید، تقاضای یک کلید پیام می‌کند. مرکز کلید، یک کلید پیام تصادفی ایجاد می‌کند و نسخه‌ای را که با کلید خصوصی الف و نسخه دیگری را که با کلید خصوصی ب رمزی‌سازی شده است برمی‌گرداند. الف پس‌ازاینکه نسخه پیام کلید خود را رمزگشایی کرد پیامش را با کلید، رمزی می‌کند و آن را همراه با نسخه کلید پیام رمزی‌شده ب به او می‌فرستد. ب کلید پیام را با کلید خصوصی خود و سپس اصل پیام را رمزگشایی می‌کند. تمام این کارها می‌تواند به‌طور خودکار انجام گیرد و بدین ترتیب نه الف و نه ب نیازی ندارند که به‌طور صریح از مرکز پیام آگاه باشند. الف فقط پیامی برای ب انشاء می‌کند و به پستچی خود دستور می‌دهد آن را رمزبندی کند. پستچی ب می‌تواند پیام الف را به‌طور خودکار رمزگشایی کند و از ب بپرسد آیا پیام الف را به‌صورت رمزگشایی می‌خواهد یا نه؟

عیب این کار این است که به شخص ثالث مورد اعتمادی نیاز است، این نیاز به شخص ثالث مورد اعتماد، به‌طور بالقوه، باعث آسیب‌پذیری است، بااین‌حال روش مذکور با موفقیت در محیط‌های کاربردی متعددی مانند بانکداری مورد استفاده قرار گرفته است.

در رویکرد چهارم از کلیدهای عمومی استفاده می‌شود.

در سال ۱۹۷۶ دو رمزنگار به نام‌های ویتفیلد دیفی[1] و پروفسور مارتین هلمن[2] در دانشگاه استانفورد روشی ابداع کردند که با آن دو طرف می‌توانند بی‌آنکه به شخص ثالث، مبادله خارج از رایانه، یا مخابره مقادیر سرّی نیاز داشته باشند، روی یک پیام سرّی توافق کنند. رالف مرکل[3] نیز مستقل از آن دو به راه‌حلی دست یافت؛ ولی در روش او در محاسبات و مخابرات، مقدار زیادی سرباز وجود داشت. دیفی و هلمن طرح خود را «سیستم توزیع کلید عمومی» نامیدند.

---

1. Withfield Diffie
2. Martin Hellman
3. Ralph Merkle

البته قبل از آن یک رمزنگار به نام جیمز الیس[1] عضو گروه امنیت الکترونیکی ـ مخابراتی سرّی دولت بریتانیا در دهه شصت روی این مفهوم کار کرده بود؛ ولی کار او تا دسامبر ۱۹۹۷ که گروه مزبور مقاله‌ای با قلم الیس و با عنوان «داستان رمزی‌سازی غیرسرّی» منتشر کرد، جزء اسناد طبقه‌بندی‌شده قرار داشت. روش دیفی ـ هلمن بر مفهوم جفت کلید خصوصی ـ عمومی مبتنی است. این پروتکل با ایجاد کلیدی خصوصی توسط هریک از طرفین به‌طور مستقل شروع می‌شود. سپس هرکدام از آنها یک کلید عمومی به‌صورت تابع ریاضی کلید خصوصی خود ایجاد می‌کنند. آنها کلیدهای عمومی را با هم مبادله، و سرانجام هر کدام از آنها، یک تابع کلید خصوصی خود و کلید عمومی طرف دیگر را محاسبه می‌کنند. روش ریاضی چنان است که هر دو طرف، به مقدار واحدی که از دو کلید خصوصی آنها گرفته شده می‌رسند. این مقدار به‌عنوان کلید پیام مورد استفاه قرار می‌گیرد.

در زمانی‌که دیفی و هلمن روش توزیع کلید عمومی خود را اختراع کردند، با مفهومی قوی‌تر که برای آن راهی پیش‌بینی نکرده بودند برخورد نمودند که آن رمزی‌نگاری کلید عمومی بود. با رمزی‌نگاری کلید عمومی، هر فرد دارای یک جفت کلید عمومی ـ خصوصی درازمدت و منحصربه‌فرد می‌شود. جزء عمومی که می‌توان آن را در اینترنت پست، و جهان را در آن شریک نمود، برای رمزی‌سازی داده‌ها مورد استفاه قرار می‌گیرد؛ ولی جزء خصوصی که محاسبه کردن آن از کلید عمومی مشکل است، در رمزگشایی مورد استفاده قرار می‌گیرد. رمزی‌نگاری کلید عمومی را «رمزی‌نگاری دوکلیدی» یا «رمزی‌نگاری نامتقارن» نیز می‌نامند. در روش‌های متعارفی نیز که در آنها از یک کلید استفاده می‌شود، رمزی‌نگاری تک‌کلیدی را رمزی‌نگاری کلید خصوصی، رمزی‌نگاری متقارن یا رمزی‌نگاری متعارف می‌نامند.

۱ـ۲ـ۴. نگهداری کلید و بازیافت: کلیدهای مورد استفاده در مخابرات موقت شامل: صدا، نمابر و انتقال داده‌ها نیاز به نگهداری ندارند؛ زیرا آنها یک‌بارمصرف شده، کنار گذاشته

1. James Ellis

می‌شوند؛ اما کلیدهایی که برای نگهداری از داده‌های ذخیره‌شده مورد استفاده قرار می‌گیرند، باید ذخیره شوند تا بتوان بعدها از داده‌ها رمزگشایی کرد. اگر این کلیدها در رایانه به‌طور روشن نگاه داشته شوند، در برابر دسترسی اشخاص غیرمجاز آسیب‌پذیر خواهند بود. آنها باید تحت یک شاه‌کلید اصلی مثل: کلید عمومی کاربر رمزی‌سازی شوند؛ ولی انجام این کار به این سؤال مربوط می‌شود که کلید خصوصی کاربر در کجا ذخیره شده است؟ با پست الکترونیکی، کلید یک پیام وارده قبلاً تحت کلید عمومی کاربر رمزی‌سازی شده و با پیام رمزی‌سازی‌شده نگهداری شده است. بنابراین آنچه مورد نیاز است، نوعی وسیله نگهداری امن کلید خصوصی کاربر است. یک راهکار برای امن نگاه داشتن کلید خصوصی، نگهداری آن در وسیله‌ای خارجی مانند کارت هوشمند یا کارت رایانه شخصی به‌نحوی است که سیستم رمزی‌سازی را بتوان به‌طورمستقیم از کارت به‌دست آورد. برای حفظ کارت در برابر استفاده غیرمجاز ممکن است از کاربر خواسته شود که برای فعال کردن کارت، کلمه عبور یا شماره شناسایی شخصی (ID) را ارائه دهد. راهکار دوم، ذخیره کردن کلید خصوصی در یک دیسک معمولی (هارد یا فلاپ) است که تحت یک کلمه عبور یا عبارت عبور که توسط کاربر تعیین شده، رمزی‌سازی شده باشد. در هر دو حالت، امنیت بالاخره به حفظ کلمه عبور یا شماره شناسایی شخصی و احتمالاً کارت بستگی دارد. موضوع دیگری که به ذخیره کلیدها مربوط است، محافظت در برابر کلیدهای گمشده یا آسیب‌دیده است. اگر کاربری کلمه عبور را فراموش کند یا وسیله‌ای که کلید خصوصی در آن نگهداری شده گم شود یا ازبین برود، رمزگشایی داده‌های ذخیره‌شده غیرممکن می‌شود. این نوع اتفاقات، غیرعادی نیست و نه‌تنها بر شخص کاربر بلکه بر کارفرمای او نیز اثر می‌گذارد.

راه دیگر حصول اطمینان بیشتر به اینکه داده‌های رمزی‌سازی‌شده در آینده در دسترس خواهند بود، استفاده از سیستم بازیافت کلید است. سیستم بازیافت کلید، پشتیبانی[1] برای

1. Back Up

به‌دست آوردن کلید رمزی‌سازی است. تسهیلات پشتیبانی می‌تواند توسط افراد و سازمان‌هایی که از رمزی‌سازی استفاده می‌کنند مدیریت شود یا مدیریت آن با شرکتی مستقل باشد. مؤسسات بسیاری خواهان توانمندی بازیافت کلید هستند؛ آنها نمی‌توانند ازدست دادن دسترسی به اطلاعات ارزشمندی را که در فایل‌های رمزی‌سازی شده ذخیره کرده‌اند تحمل کنند. به‌همین‌دلیل این امر به موضوع مهمی در سیاست رمزی‌سازی ملی تبدیل شده است. در بیشتر سیستم‌های بازیافت کلید اصلی، کلیدهای اصلی بایگانی می‌شوند؛ ولی یکایک کلیدهای پیام، بایگانی نمی‌شوند. یک کلید موجود در آرشیو می‌تواند کلید خصوصی کاربر یا یک کلید خصوصی باشد که در محصول رمزی‌سازی، جاسازی شده و فقط برای بازیافت کلید مورد استفاده قرار می‌گیرد. کلید هر فایل یا پیام پست الکترونیک درقالب جزء عمومی این کلید رمزی‌سازی می‌شود و سپس ذخیره یا همراه داده‌ها مخابره می‌شود. وقتی شخص مجازی نیازمند دسترسی به پیام‌هایی که به کاربر ارسال شده یا داده‌های ذخیره‌شده در رایانه کاربر است، عامل بازیافت به رمزگشایی کلیدهای پیام کمک می‌کند یا نسخه‌ای از کلید بازیافت را در اختیار او می‌گذارد؛ ولی کلید اصل مرکز، کلید بازیافت را به وی نمی‌دهد تا بتواند بدون کمک بیشتر داده‌ها را بازیافت کند. سیستم‌های شخص ثالث که کلیدهای خصوصی کاربران یا محصولات آنها را نزد شخص ثالث قابل اعتمادی در آرشیو قرار می‌دهند، گاهی سیستم‌های کلید امانی[1] نامیده می‌شوند؛ ولی عبارت کلید امانی گاهی به‌همان معنای بازیافت کلید به‌کار می‌رود. چون شاه‌کلید یا کلید اصلی ماهیت حساسی دارد، آن را بین دو یا چند نفر تقسیم می‌کنند. بدین‌ترتیب هیچ فرد واحدی نمی‌تواند به‌تنهایی کلید را به‌مخاطره اندازد. برای کامل بودن کلید، تمام کلیدداران باید با هم تشریک مساعی کنند. بخش‌های شاه‌کلید را می‌توان در تأسیسات مطمئن جداگانه تحت کنترل اشخاص مختلف ذخیره کرد. در دنیای دیجیتال، یک کلید سرّی K را به سادگی به دو نیمه X و Y تقسیم می‌کنند و این تقسیم به‌گونه‌ای است که

---

1. Key Escrow

هیچ‌کدام از دو نیمه نمی‌تواند برای دستیابی به نیمه دیگر یا کل کلید مورد استفاده قرار گیرد.

۵. کاربرد رمزی‌سازی: از رمزگشایی می‌توان برای محافظت از داده‌های ذخیره‌شده شامل: فایل‌های کامل یا اجزاء فایل، و مخابرات شامل: مکالمات تلفنی، نمابر، پست الکترونیکی، معاملات شبکه‌ای، معاملات بانکی، شبکه‌های اضافی شرکت‌ها و سایر کاربردهای شبکه استفاده کرد. بعضی از سیستم‌های رمزی‌سازی، همه چیز را در دیسک سخت رمزی‌سازی می‌کنند؛ به‌طوری‌که در صورت ندانستن کلید رایانه، قابل استفاده مؤثر نیست. دیسک‌های کامل و فایل‌های رمزبندی‌شده به‌ویژه با رایانه‌های کیفی[1] مفید هستند. اگر رایانه دزدیده شود، داده‌های حساس درمعرض استفاده قرار نمی‌گیرند. رمزی‌سازی به‌صورت اجزای نرم‌افزار و نیز سخت‌افزار موجود است و می‌توان آن را به‌صورت دستگاه‌های رمزی‌سازی تنها، بسته‌های نرم‌افزاری یا به‌صورت ویژگی محصولات دیگر دریافت کرد.

بسیاری از کاربردهای نرم‌افزار و برنامه‌های بهره‌برداری از رمزی‌سازی پشتیبانی می‌کنند. نرم‌افزارهای رایانه‌ای به‌طور فزاینده با رمزی‌سازی قرارگرفته‌شده در داخل همراه می‌شوند. ارتباطات می‌تواند یا «رمزی‌شده انتها به انتها»[2] یا «رمزی‌شده پیوند»[3] باشد. در رمزی‌شده انتها به انتها، صرف‌نظر از اینکه پیام چند رایانه یا پیوند را طی می‌کند، بین نقاط انتهایی یک پیام، کانالی مطمئن ایجاد می‌شود. رمزی‌سازی پیوند، پیام را در طول پیوند یا شبکه‌ای فرعی محافظت می‌کند، اما نه در تمام مسیر. مزیت آن این است که لازم نیست هر دو نقطه انتهایی از رمزی‌سازی پشتیبانی کنند یا رمزی‌سازی هر دو انتها با هم سازگار باشند. سیستم جهانی تلفن همراه GSM[4] ـ که در سرتاسر جهان برای مخابرات سلولی دیجیتالی مورد استفاده است ـ برای محافظت از پیوند هوایی بین یک تلفن همراه و یک ایستگاه کاری از رمزی‌سازی پیوند استفاده می‌کند. صرف‌نظر از اینکه فردی که در طرف دیگر مکالمه قرار دارد از تلفن سلولی

---

1. Qualified Computers
2. End to End Encrypted
3. Link Encrypted
4. Global System for Mobil

استفاده می‌کند یا از سیستم جهانی تلفن همراه، پیوند بدون سیم رمزی‌سازی می‌شود.

بین ایستگاه‌های کاری، مخابرات از شبکه تلفن عمومی می‌گذرد و بخش‌های آن ممکن است به‌طورمستقل رمزی شده یا نشده باشند. در پاره‌ای از دستگاه‌های تلفن مطمئن از رمزی‌سازی انتها به انتها استفاده می‌شود. رمزی‌سازی کاربردی رایج به‌نام «شبکه‌های خصوصی مجازی» (SVPN) دارد. این شبکه تأسیسات یک مؤسسه را که ازنظر جغرافیایی پراکنده هستند در شبکه‌ای عمومی مثلاً اینترنت یا سرویس رله‌قابی (At & T) به‌هم مربوط می‌کند. شبکه خصوصی مجازی اساساً برای کل مؤسسه، ارتباطات جهانی مطمئن تأمین می‌کند، بی‌آنکه نیازی به خطوط اجاره‌ای خصوصی باشد. شبکه خصوصی مجازی ممکن است با یک سخت‌افزار اختصاصی یا نرم‌افزار اجرا شود یا در یک فایروال[1] ادغام گردد و برای تأمین ارتباطات رمزی‌شده فایروال یا فایروال به ارتباطات کاربر دور مورد استفاده قرار گیرد. محصولات فایروالی تجاری متعددی از شبکه‌های خصوصی مجازی پشتیبانی می‌کنند. شبکه خصوصی مجازی، جانشین ارزان‌تر خطوط اجاره‌ای است. بیشتر محصولات این شبکه از تکنیکی به نام «تونل زدن» پشتیبانی می‌کنند. این تکنیک، سرصفحه و محتوای بسته را رمزی‌سازی می‌کند و سپس آنها را قبل از ارسال کردن در سرصفحه جدید می‌پیچد.

رمزی‌سازی را می‌توان در یک تراشه ریزپردازنده که در کارت هوشمند یا سایر دستگاه‌ها ذخیره شده انجام داد. کارت‌های هوشمند، درست مثل کارت‌های اعتباری است که در تراشه‌های کوچک آنها اطلاعات ذخیره و برنامه‌ها اجرا می‌شوند. کارت‌ها می‌توانند حجم عظیمی از اطلاعات را شامل شوند؛ مثل: سوابق کامل پزشکی شخص. می‌توان برای محافظت از اطلاعات قرار داده‌شده در کارت، از رمزی‌سازی استفاده کرد. می‌توان پلاک کوچکی را که سربازان درحال انجام وظیفه بر گردن دارند، با پلاک‌هایی فناوری بالا تعویض کرد. پلاک‌های کوچک قدیمی حاوی فقط پنج خط اطلاعات (نام، مذهب و گروه خون) هستند؛ ولی

---

1. Firewall

پلاک‌های دیجیتالی جدید حاوی حجم عظیمی از اطلاعات مانند: تاریخچه پزشکی، اشعه ایکس و نتایج نوار قلب خواهند بود. پرسنل پزشکی در جبهه‌ها، با دستگاه دستی کوچک یا رایانه کیفی، اطلاعات این تراشه‌های رایانه‌ای را خواهند خواند و در درمان سربازان مجروح از آن اطلاعات استفاده خواهند کرد. این اطلاعات رمزی‌سازی شده‌اند؛ ولی نگرانی‌هایی وجود دارد که اگر رمز این اطلاعات شکسته شود و پلاک دست دشمن بیفتد، چه اتفاقی ممکن است رخ دهد.

۱ـ۲ـ۶. محدودیت‌های رمزی‌سازی: رمزی‌سازی روشی نیرومند برای محافظت از داده‌های درحال انتقال یا ذخیره‌شده در رایانه است. این داده‌ها در برابر تحقیقات محرمانه یا تصرف آسیب‌پذیر هستند. با این توصیف، روش مذکور دو محدودیت اساسی دارد: اول اینکه، نمی‌تواند از داده‌ها در زمانی‌که مورد پردازش رایانه قرار دارند محافظت کند. علت این است که داده‌ها برای اینکه رمزی‌سازی شوند، باید دارای نظم روشنی باشند. اگرچه این امکان وجود دارد که سیستم‌های رمزی‌سازی را طوری طراحی کرد که انجام عملیات بر متن رمزی‌شده ممکن باشد، این نوع سیستم‌ها یا ضعیف خواهند بود یا قابلیت عملیاتی بسیار محدود خواهند داشت. پیامد پردازش داده‌ها در حالت غیررمزی‌شده آنها این است که اگر یک متجاوز به رایانه دسترسی پیدا کند می‌تواند داده‌های حساس را در زمان تایپ یا پردازش شدن بردارد. یک راه این سرقت، استفاده از یک برنامه تجسس صفحه کلید است؛ مانند آنچه در ژانویه ۱۹۹۶ توسط شرکت First Virtual Holdings نشان داده شد. آن برنامه، زدن دکمه برای شماره‌های کارت اعتباری را کنترل می‌کرد و وقتی متوجه می‌شد که شماره کامل تایپ شده، موسیقی نامناسبی می‌نواخت و دریچه‌ای بیرون می‌داد که در آن، شماره کارت و تایپ آن نشان داده می‌شد. در اصل، این برنامه می‌توانست شماره‌ها را با اینترنت به شخص ناشناخته‌ای انتقال دهد؛ ولی هدف شرکت مذکور تقلب نبود. آنها می‌خواستند نشان دهند که فرستادن شماره کارت‌ها به‌صورت رمزی‌سازی‌شده کافی نیست؛ امنیت باید از صفحه کلید شروع شود.

اگر خود رمزی‌سازی به‌جای‌اینکه روی کارت هوشمند جداگانه یا سایر دستگاه‌ها انجام

گیرد روی خود رایانه انجام شود، متجاوز حتی قادر خواهد شد کلیدهای رمزی‌سازی را در جریان استفاده بردارد.

رمزی‌سازی را اغلب برای امنیت اطلاعات به‌صورت «گلوله نقره‌ای» نمایش داده‌اند که متأسفانه واقعیت با آن تفاوت بسیار دارد. رمزی‌سازی در برابر اکثر حملات ازجمله سوءاستفاده داخلی‌ها (خودی‌ها)، مهندسی اجتماعی، وارد شدن به سیستم از نقاط آسیب‌پذیر آن، دست‌کاری داده‌ها، تروجان‌ها، ویروس‌ها، خال‌های وب و بیشتر حملات مانع سرویس، محافظتی ارائه نمی‌دهد. رمزی‌سازی چیزی جز یک عنصر برنامه نبرد اطلاعاتی دفاعی نیست.

۱ـ۳. سرّی‌نگاری

سرّی‌نگاری، نوعی مخفی کردن پیام است، بدون آنکه اصل پیام دچار تغییر گردد. این کار با قرار دادن پیام در داخل یک سند، تصویر، نوار صوتی یا ویدئویی انجام می‌گیرد. هرکس که بداند آن واسط، حاوی یک پیام سرّی است، اگر روش رمز گذاشتن (و احتمالاً یک کلید سرّی) را بداند می‌تواند پیام را استخراج کند؛ ولی آن پیام، برای هرکس دیگری کاملاً نامرئی است.

دیوید کاهن[1] در کتاب «رمزشکنان» موارد استفاده از سرّی‌نگاری در گذشته‌های دور را ذکر کرده است. در یک مورد ـ که در تاریخ هرودوت مستند شده ـ دماراتوس می‌خواست به اسپارتی‌ها اطلاع دهد که خشایارشاه درحال برنامه‌ریزی برای حمله به یونان است. دماراتوس برای رساندن پیام بی‌آنکه در راه کشف شود، موم روی چند لوح چوبی تاشو را تراشید، پیام خود را روی چوب نوشت و سپس آن را دوباره با موم پوشاند. وقتی لوح‌ها به مقصد رسید، هیچ‌کس اهمیت آن را نمی‌دانست تا اینکه زنی به نام گورگو متوجه موضوع شد.

ازجمله روش‌های دیگر پنهان کردن عبارتند از: نوشتن با جوهر نامرئی و ریزنقطه[2].

---

1. David Kahen
2. Microdots

ریزنقطه، عکس‌هایی به اندازه یک نقطه است که یک صفحه کامل تایپ‌شده را به وضوح تمام نشان می‌دهد. در جنگ جهانی دوم، آلمانی‌ها که مبدع این فناوری بودند، صدها ریزنقطه را در جاهای خالی تلگراف‌ها، نامه‌های عاشقانه مکاتبات تجاری و نامه‌های خانوادگی قرار دادند.

یکی دیگر از روش‌های سرّی‌نگاری، قرار دادن پیام در داخل تصویر دیجیتال است. این تصویرها با آرایه‌ای از تصویر ـ دانه‌ها (پیکسل‌ها) که مطابق نقطه‌های تصویر است نمایانده می‌شوند. یک تصویر خوب دارای ۲۰۴۸ × ۳۰۷۲ تصویر ـ دانه است و تصویری با دقت کمتر ممکن است از ۴۰۰×۳۰۰ تصویر ـ دانه درست شده باشد. هر تصویر ـ دانه با تعدادی بیت که تعیین‌کننده رنگ آن است احاطه شده است. این رمزبندی در ساده‌ترین شکل خود، مقدار ۲۴ بیتی است که در آن هشت بیت اول مشخص‌کننده رنگ قرمز، دومین هشت بیت مشخص‌کننده رنگ آبی، و سومی مشخص‌کننده رنگ زرد است. این قلعه‌های هشت بیتی ـ که بایت نامیده می‌شوند ـ در ترکیب با هم ۲۵۶ گونه مختلف را ممکن ساخته، تقریباً هفده میلیون رنگ ممکن ایجاد می‌کنند. این مطلب، در مقایسه با آنچه احتمالاً در منبع تصویر وجود دارد و آنچه می‌توان در یک صفحه نمایش (مونیتور) رنگی دید، دقت رنگ بسیار بیشتری را ممکن می‌سازد (دوربین‌های دیجیتال و پویشگرهای تصویر، دقیق نیستند). بنابراین می‌توان برای رمزبندی کردن یک پیام سرّی، بعضی از بیت‌ها را «مصادره» کرد، بی‌آنکه بر تصویر اثر بگذارند. بیشتر فایل‌های تصویر که در اینترنت توزیع می‌شوند تصویر ـ دانه‌ها را با ۲۴ بیت رمزبندی نمی‌کنند، بلکه در آنها از نمایش فشرده‌تری استفاده می‌شود. نتیجه توجه به این واقعیت است که در بسیاری از عکس‌ها، تعداد رنگ‌های مورد استفاده بسیار کمتر از هفده میلیون رنگ است (شاید فقط یک مشت رنگ باشند)؛ برای مثال، فرمت GIF هر تصویر ـ دانه را فقط با یک بایت در میزرنگ رمزبندی می‌کند. میزرنگ دارای تا ۲۵۶ رنگ مختلف است که از تصویر اصلی گرفته می‌شود. از GIF و سایر فرمت‌های فشرده مانند JPEG می‌توان برای پنهان کردن پیام‌ها استفاده کرد؛ اما این فرایند، دشوارتر است. برای مخفی کردن پیام‌ها در

فایل‌های تصویری و صوتی، در اینترنت ابزارهای متعددی وجود دارند. با اس ـ تولز[1] می‌توان فایل سندی را به سادگی با کشاندن نماد تصویری[2] بر روی تصویر، در تصویر پنهان کرد. از کاربر خواسته می‌شود یک کلمه عبور معین کند، سپس باید فایل را از تصویر بیرون کشید. اگر امنیت بیشتری موردنظر باشد، می‌توان پیام را اول رمزی‌سازی کرد. به سختی می‌توان متوجه تفاوت بین تصویرهای قبلی و بعدی شد. اس تولز، بیت‌ها را در فضای خالی دیسکت هم مخفی می‌کند، ولی این محل جای امنی برای ذخیره کردن پیام نیست؛ زیرا اگر سیستم عامل، فضا را به فایل دیگر اختصاص دهد، ممکن است چیز دیگری روی آن ضبط شود. ازآنجاکه هر بیت یک پیام، به‌طور مؤثری در لای چند بیت میزبان قرار گرفته است، سرّی‌نگاری وسیله کارآمدی برای ارسال پیام سرّی نیست. در مقایسه با رمزی‌نگاری، پیام سرّی‌شده تقریباً مشابه پیام ساده رمزی‌نشده است.

سرّی‌نگاری همچنین ممکن است از امنیت بسیار کمتری برخوردار باشد (حداقل اگر کلیدبندی نشود و با رمزی‌نگاری مورد استفاده قرار نگیرد). ازطرف‌دیگر سرّی‌نگاری می‌تواند صرفاً وجود پیام مخفی را در درون آنچه متن ساده به‌نظر می‌رسد پنهان کند. یک فایل تصویر را می‌توان به سرور وب پست کرد و برای عموم قابل دسترس ساخت و فقط ممکن است تعداد کمی از افراد درباره سرِّ پنهان چیزی بدانند؛ چون کشف کردن آن مشکل است. سرّی‌نگاری می‌تواند برای تضعیف قواعد یا سیاست‌های شرکت که به رمزی‌سازی حاکم است مورد استفاده قرار بگیرد.

سرّی‌نگاری برای پنهان کردن فعالیت مجرمانه مورد استفاده قرارگرفته است؛ برای مثال، یک دزد کارت اعتباری برای پنهان کردن شماره‌های کارت‌های سرقتی در صفحه مورد تجاوز قرارگرفته وب از سرّی‌نگاری استفاده می‌کرد. او گلوله‌های روی صفحه (دایره‌های کوچک توپر) را با تصاویری که مثل همان گلوله‌ها به‌نظر می‌رسید، ولی حاوی شماره‌های کارت‌های

---

1. S-Tools
2. Icon

اعتباری بود جایگزین کرد. این مورد، پتانسیل استفاده از تصاویر وب به‌عنوان «قطره‌های دیجیتال مرده» را برای واسطگی اطلاعات نشان می‌دهد. از سرّی‌نگاری می‌توان برای پنهان کردن وجود فایل‌ها در دیسک سخت رایانه استفاده کرد.

۱ـ۴. گمنام‌سازی

می‌توان با انجام اقداماتی به‌طور ناشناس، مثلاً با نقدی خرید کردن، انداختن پیام بی‌امضا به صندوق پیشنهادات و تلفن کردن از یک تلفن پولی (عمومی)، تهدیدهایی را که متوجه حریم خصوصی است کاهش داد. اگر هویت مشتری نامعلوم باشد، بخش بازرگانی یک شرکت نمی‌تواند شرح عادات خرید را تهیه کند یا به یک شرکت بازاریابی، نام و الگوهای خرید را بفروشد. اگر یک مرکز بحران نداند چه کسی به تلفن سرخ زنگ زده، خطراتی که کسی از آن اطلاعات سوءاستفاده کند وجود ندارد.

در اینترنت مردم به‌وسیله تأمین‌کننده سرویس اینترنت خود و نشانی‌های پست الکترونیکی خود شناخته می‌شوند. یک راه مخفی کردن این اطلاعات، استفاده از دوباره پست‌کننده‌های بی‌نام است. الف برای فرستادن پیام ایمیلی به ب، پیام را به یک سرور ایمیل می‌فرستد. سرور ایمیل، سرفصل‌ها را برمی‌دارد و پیام را به ب ارسال می‌کند. ب با دریافت پیام، درمی‌یابد که پیام ازطریق سرور ایمیل ارسال شده است؛ اما نمی‌تواند پی ببرد که فرستنده چه کسی بوده است. بعضی از سرورهای ایمیل به کاربر اسم مستعار می‌دهند تا دریافت‌کنندگان بتوانند ازطریق این سرورها به پیام جواب بدهند. سرورها نیز جواب‌ها را به صاحبان اسامی مستعار ارسال می‌کنند. این سرورها گمنام‌سازی کامل را تأمین نمی‌کنند؛ زیرا خود آنها طرفین پیام را می‌شناسند. تنها کار آنها این است که نقش یک پستچی را ایفا می‌کنند.

یک سرور ایمیل می‌تواند پیام‌ها را قبل از ارسال به مقصد روی هم انباشته کند. با این عمل اگر کسی به‌منظور تجزیه‌وتحلیل ترافیک به پیام‌های رمزی‌شده اینترنت دستبرد بزند، نمی‌تواند بفهمد چه کسی با چه کسی صحبت می‌کند. کاربرانی که به سرورهای ایمیل اعتماد ندارند

می‌توانند پیام‌های خود را ازطریق چند سرور ارسال کنند.

در وب کاربران می‌توانند به‌طور ناشناس با رفتن به سایتی که این قابلیت را تأمین می‌کند به اطلاعات دسترسی پیدا کنند. آنها وقتی می‌خواهند از وب سایت خاصی دیدن کنند، سه حرف URL را در رمزی که توسط «بی‌نام‌کننده»[1] ارائه می‌شود تایپ می‌کنند. آنگاه فرم پاک، و صفحه باز می‌شود. با این عمل، سایت‌هایی که مورد بازدید آنها قرار می‌گیرند، نمی‌توانند بدانند که مراجعه‌کننده چه کسی بوده است. بعضی از سایت‌ها، خدمات پست الکترونیکی با نام مستعار را ارائه می‌دهند. کاربر می‌تواند پیام را در یک فرم تایپ کند، سرور ایمیل را انتخاب و پیام را ارسال نماید.

خرید نقدی، سازوکاری برای انجام خریدهای ناشناس است؛ ولی این سازوکار، ناشناس ماندن را تضمین نمی‌کند؛ زیرا ممکن است فروشنده خریدار را بشناسد یا تصویر خریدار با دوربین ویدئویی ضبط شده باشد. بااین‌وصف مشتریان می‌توانند در معاملات نقدی، در مقایسه با خرید با چک یا کارت اعتباری که هویت خریدار به وضوح مشخص می‌شود بیشتر ناشناس بمانند.

نقد کردن دیجیتالی[2] همان خاصیت خصوصی بودن پول نقد را دارد؛ ولی درعین‌حال از خرید الکترونیکی پشتیبانی می‌کند. بعضی روش‌ها، بی‌نام‌ونشان ماندن مطلق را تأمین می‌کنند، درحالی‌که در مورد بعضی دیگر، ردیابی کردن خریدار در شرایط محدود (مثلاً دستور دادگاه) ممکن است. بعضی به‌صورت کارت‌های پیش‌پرداخت مکالمات تلفنی یا خریدهای کلی‌تر (معمولاً در خارج از شبکه) انجام می‌گیرند. برای پرداخت با اینترنت، برخی سیستم‌ها ازجمله نقد الکترونیکی توسط شرکتی[3] در آمستردام هلند ابداع شده است. برای استفاده از این سیستم، هم فروشنده و هم خریدار باید در بانکی که از آنها پشتیبانی می‌کند، حساب دسترسی ارز جهانی داشته باشند. خریداران، پول را از حساب‌های خود به ضرابخانه نقد الکترونیکی[4] انتقال می‌دهند و از آنجا نقد الکترونیکی برای خرید کردن برداشت می‌شود. جهت محافظت در برابر

---

1. Anonymizer
2. Digital Cash
3. Digi Cash
4. E-cash Mint

تقلب و نیز تضمین بی‌نام‌ونشان ماندن، از رمزی‌سازی استفاده می‌شود. از گمنام‌سازی هم می‌توان به‌نحو مطلوب یا نامطلوب استفاده کرد.

۱ـ۵. بهداشتی کردن

بهداشتی کردن راهی برای انتشار مطالبی است که از اطلاعات حساس استخراج شده، ولی خود آن اطلاعات را برملا نمی‌کند؛ برای مثال، ادارات سرشماری و مؤسساتی که نظرسنجی انجام می‌دهند، آمارهای کلی نظرسنجی‌های خود را منتشر می‌کنند؛ ولی اطلاعات مربوط به تک‌تک شهروندان یا شرکت‌ها را محرمانه نگاه می‌دارند. مؤسسات تجاری در مورد محصولات خود نوشته‌ها و بیانیه‌های مطبوعاتی انتشار می‌دهند؛ اما اسرار تجاری را که پشت آن محصولات قرار دارد برملا نمی‌کنند. دولت‌ها گزارش‌های طبقه‌بندی‌شده را با سیاه کردن آن قسمت‌هایی که حساس است به‌صورت اسناد طبقه‌بندی نشده منتشر می‌کنند.

فرایندهایی که اطلاعات را بهداشتی می‌کنند و از صافی می‌گذرانند، نه فقط باید مانع برملا شدن مستقیم اطلاعات حساس شوند، بلکه باید مانع افشاء غیرمستقیم ازطریق استنتاج و جمع‌بندی اطلاعات منابع دیگر نیز باشند. در غیراین‌صورت انتشار گزارش‌های بهداشتی‌شده می‌تواند موجب تضعیف امنیت اطلاعاتی شود. ادارات سرشماری، برای محافظت در برابر افشاء ناخواسته و حملات هماهنگ به بانک‌های اطلاعاتی و آمارهای منتشره روش‌های ویژه‌ای طراحی و اجرا می‌کنند.

یکی از مشکلات موجود این است که اطلاعاتی که به تنهایی طبقه‌بندی‌شده نیستند، ممکن است درصورت یکپارچگی، به اطلاعات نیازمند طبقه‌بندی تبدیل شوند؛ برای مثال ممکن است دو نفر یک یا چند سند مربوط به هم را بهداشتی کنند و گزارش‌هایی تهیه نمایند که به تنهایی طبقه‌بندی‌شده نیستند؛ اما به‌طورکلی اطلاعات طبقه‌بندی‌شده‌ای را برملا می‌کنند. جلوگیری از این نوع افشاها فوق‌العاده مشکل است.

۱ـ۶. دفع آشغال

روش صحیح خلاص شدن از زباله و آشغال ازجمله ریز ریز کردن کاغذ می‌تواند اطلاعات حساس را از داخلی‌هایی که ظرف زباله اداره را زیرورو می‌کنند و خارجی‌هایی که به ظرف‌های بزرگ زباله شیرجه می‌روند محافظت کند. ولی خرد کردن کاغذ همیشه با موفقیت همراه نیست؛ چون دستگاه‌هایی آنها را بازسازی می‌کنند.

آشغال‌های آنلاین هم باید به‌نحو صحیح دفع شوند تا افراد غیرمجازی که در همان منابع رایانه‌ای سهیم هستند یا زیروروکنندگان ظرف‌های زباله بیرون که رایانه‌ها و دیسکت‌های دورانداخته شده را برمی‌دارند، به آنها دسترسی پیدا نکنند. منطقه‌ای که داده‌ها بیشتر از دیگر مناطق در آنها آسیب‌پذیرند، حافظه اصلی سرورها هستند. اگر سیستم عامل قبل از محول کردن کاربر جدید به یک بلوک حافظه، آن بلوک را پاک نکند، ممکن است کاربر جدید کلمات عبور، کلیدهای رمزی‌سازی و سایر داده‌های حساسی را که پشت برنامه قبلی قرار دارند بردارد. متأسفانه بسیاری از سیستم عامل‌ها چنین هستند و پاک کردن را به عهده خود نرم‌افزار می‌گذارند. همین مشکلات در مورد فضای دیسک که به فایل‌ها اختصاص می‌یابد نیز وجود دارد.

داده‌های ذخیره‌شده در دیسکت، حتی پس از پاک شدن نیز آسیب‌پذیر هستند. وقتی فایلی پاک می‌شود، بیت‌ها در واسط ذخیره آن‌قدر باقی می‌مانند که بیت تازه‌ای روی آنها نوشته شود. حتی پس از این نیز اگر داده‌ها به اندازه کافی پاک نشده باشند، قابل بازیافت هستند.

۱ـ۷. سپرسازی

سپرسازی راه دیگر پنهان کردن اطلاعات است. در محیط فیزیکی، تأسیسات محرمانه را می‌توان در زیرلایه‌ای از استتار پنهان کرد. هواپیماها و ماهواره‌های جاسوسی و سلاح‌ها را می‌توان با سپر ضدکشف راداری پوشاند و گیرنده‌های رادار را فریب داد. می‌توان تلفن‌های عمومی پولی یا ماشین‌های خودپرداز بانک‌ها را نیز دارای سپر کرد تا کمک کند کسانی که از

روی حرکت شانه‌ها، شماره تلفن و شماره کارت بانک را هنگام فشردن دکمه‌ها به‌دست می‌آورند در قصد خود موفق نشوند.

رایانه‌ها و سایر تجهیزات الکترونیکی هم می‌توانند برای محافظت از خود در برابر برخی گیرنده‌های خاص روی وانت که تشعشعات الکترومغناطیسی آنها را می‌گیرند، از سیستم TEMPEST استفاده کنند. تجهیزات یا در ظرف مخصوصی که دارای سپر الکترومغناطیسی است گذاشته می‌شوند یا طوری مهندسی می‌شوند که سیگنال‌ها در همان منبع خود ازبین بروند. ازبین بردن سیگنال‌ها در منبع خود، ازنظر فنی مشکل‌تر است؛ اما محدودیت‌های کمتری بر چگونگی استفاده از تجهیزات تحمیل می‌کند. فناوری TEMPEST به‌شدت تحت کنترل قرار دارد و استانداردهای آن طبقه‌بندی‌شده هستند.

۲. روش‌های تأیید اعتبار

تأیید اعتبار، فرایند تعیین این امر است که اطلاعات، قابل اعتماد و اصل است یا فاسد و جعل‌شده. سازوکار تعیین اینکه داده‌ها دست‌کاری شده یا به منبع نادرستی منسوب شده‌اند نیز بخشی از فرایند تأیید اعتبار است. فرایند مذکور شامل اقدامات غیررایانه‌ای و برنامه‌های رایانه‌ای است که به‌ترتیب در جهان فیزیکی و فضای رایانه‌ای انجام می‌گیرند.

تأیید اعتبار در برابر اقداماتی که یکپارچگی را تضعیف می‌کند (مانند: تلف کردن وقت با داده‌ها و جعل اسناد و پیام‌ها) محافظت را تأمین می‌کند؛ ولی چون به‌عنوان وسیله کنترل دسترسی به منابع اطلاعات به‌کار می‌رود، به‌طور غیرمستقیم در برابر سایر اقدامات غیرمجاز ازجمله: سرقت اطلاعات حساس و حملات مختل‌کننده سرویس‌ها نیز از اطلاعات مربوطه محافظت می‌نماید.

تأییدکننده‌های اعتبار، چهار نوع اصلی هستند: نوع اول، اطلاعاتی است که ذاتاً در موجودیت تحت بررسی (برای تأیید اعتبار) وجود دارد. مشخصات شخصی مانند: ظاهر، صدا، خط و خواص ممیزه اسناد براساس ظاهر و محتوای آنها ازجمله این نوع اطلاعات است. نوع

دوم، رمزی مانند: کلمه عبور، شماره هویت شخصی[1]، کلید رمزی‌نگاری یا سایر قطعه‌های اطلاعات است. نوع سوم، دارا بودن اشیایی مانند: پلاک شناسایی، رمز دسترسی، کارت اعتباری یا شماره تلفن است. نوع چهارم، محل فیزیکی تمامیت یا بخشی از اطلاعات است. در بسیاری از روش‌های تأیید اعتبار، ترکیبی از این چهار نوع مورد استفاده قرار می‌گیرد؛ مثلاً ممکن است همراه با کارت‌بانک، شماره هویت شخصی مخفی نیز مطالبه شود.

۲ـ۱. زیست‌سنجی

مدت‌ها قبل از اینکه رایانه اختراع شود، مردم خود را براساس ظاهر و صدا به یکدیگر می‌شناساندند. آنها به حافظه خود و شرحی که دیگران می‌دادند اتکا می‌کردند تا پی ببرند شخصی که با آن روبه‌رو شده‌اند همان کسی که ادعا می‌کند هست یا نه. اختراع عکاسی، ثبت ظاهر بر روی ورقه کاغذ را ممکن ساخت. در نتیجه، افرادی را هم که کاملاً غریبه بودند می‌شد شناسایی کرد. تشخیص هویت از روی عکس هنوز هم به‌طور معمول توسط مقامات مهاجرت که ورود افراد را در مرزها کنترل می‌کنند، مقامات پلیس که جریمه رانندگی را صادر می‌کنند، بازرگانانی که چک شخصی صادر می‌کنند و سازمان‌هایی که ورود افراد به ساختمان‌های خود را کنترل می‌کنند انجام می‌گیرد.

کشف ویژگی‌های اثر انگشت، تعیین هویت و شناسایی اشخاصی را که در صحنه جنایت به اشیاء دست زده‌اند ممکن ساخت. سپس شناسایی از روی DNA که روش فوق‌العاده دقیقی از تطبیق دادن شواهد موجود در صحنه جنایت با ویژگی‌های منحصربه‌فرد مشخص است، مورد استفاده قرار گرفت. این روش نه‌تنها برای محکوم کردن متهم استفاده می‌شود، بلکه با استفاده از آن، کسانی که به اشتباه به جرم‌هایی مانند: قتل یا تجاوز به عنف محکوم شده‌اند از زندان آزاد می‌شوند. احتمال خطای روش مذکور که از سال ۱۹۸۸ به‌بعد در محاکمات جنایی

1. PIN

مورد استفاده قرار گرفت، حدود یک در دویست میلیارد است.

در سال‌های اخیر انواع مشخصات زیست‌شناختی برای ساختن دستگاه‌های خودکار تأیید اعتبار مورد استفاده قرار گرفته‌اند؛ اثر انگشت، اثر صدا، الگوهای عنبیه و شبکیه چشم، الگوهای صورت و غیره ازجمله این مشخصات هستند. در یک سناریو، شخصی به طرف دستگاهی که دارای دریافتگرهای اندازه‌گیری مشخصات موردنظر است حرکت می‌کند. آنچه دستگاه می‌خواند رقمی می‌شود و با آنچه قبلاً در رایانه یا حافظه پلاکی که توسط آن شخص حمل می‌شود، ذخیره و مقایسه می‌گردد. اگر آنچه دستگاه خوانده در محدوده خطای مجاز اندازه‌گیری باشد یا با نوسانات جزئی آن مشخصات مطابقت داشته باشد پذیرفته شده، و در غیراین‌صورت رد می‌شود.

روش‌های زیست‌سنجی بر سایر انواع تأیید اعتبار، چند برتری دارند. این روش‌ها بهتر از سایر سازوکارها به‌ویژه کلمه عبور، اثبات‌کننده هویت هستند و کاربر نیازی به حفظ کردن چیزی در حافظه خود ندارد. از این روش‌ها می‌توان هم برای تعیین هویت و هم برای تأیید آن استفاده کرد. پس‌ازاینکه قرائت اثر انجام شد، سیستم می‌تواند برای مطابقت، یک بانک اطلاعاتی را جست‌وجو کند. درضمن، از یک تأییدکننده اعتبار می‌توان در همه جا استفاده کرد. درحال‌حاضر افراد مجبورند دوجین شماره شناسایی و کلمه عبور را هنگام استفاده از رایانه و دسترسی به سایت‌های موردنظر در حافظه خود داشته باشند. به‌علاوه هر وقت سایت تازه‌ای را می‌بینند که نیاز به ثبت دارد، مجبورند نام، نشانی پست الکترونیکی و سایر اطلاعات شناسایی خود را تایپ کنند. خیلی راحت‌تر بود که دوربین کوچکی روی رایانه (یا یک دستگاه قرائت اثر انگشت، روی صفحه کلید) نصب می‌شد که مشخصات را پویش (اسکن)، و از آنها برای شناسایی و تأیید اعتبار در همه جای شبکه استفاده می‌کرد. امضای دیجیتالی ـ که بعداً مورد بحث قرار خواهد گرفت ـ دارای مزیت مشابهی است. ولی یک ایراد به‌کار بردن وسیع هرکدام از این روش‌ها این است که شناسانده‌ای همه‌جایی به‌وجود می‌آورد. اگر در همه‌جا از مشخصات فیزیکی یا شناسانده‌های دیجیتالی واحدی استفاده شود، اطلاعات مربوط به یک شخص را می‌توان از

سایت‌های متعدد به‌دست آورد و با تلفیق آنها، شرحی از فعالیت‌های آن شخص تهیه نمود.

عیب روش‌های زیست‌سنجی این است که در مقایسه با سایر روش‌های تأیید اعتبار مثل کلمه رمز، نسبتاً گران هستند (البته با کامل‌تر شدن فناوری و رواج آن قیمت‌ها پایین می‌آید). به‌علاوه در این روش‌ها تجهیزات ویژه‌ای لازم است که به‌طور بالقوه در معرض آسیب قرار دارند.

رمزهای زیست‌سنجی مانند انواع دیگر شناسایی هویت (شماره تأمین اجتماعی) به‌طور بالقوه در معرض سرقت و سوءاستفاده قرار دارند؛ برای مثال، اثر انگشت دیجیتالی را می‌توان در اینترنت فروخت یا بدون اعلام کردن جمع‌آوری کرد.

۲ـ۲. کلمه‌های عبور

بسیاری از سیستم‌های تأیید اعتبار و کنترل دسترسی، به سیستم‌هایی مانند: ترکیبی از قفل‌ها، رمزهای دسترسی در درها، کلمه‌های عبور و شماره شناسایی شخصی (PIN) مبتنی هستند. این اطلاعات را می‌توان در دستگاه‌هایی فیزیکی مانند پلاک دسترسی، کارت هوشمند یا دیسکت رایانه‌ای به حافظه سپرد یا ذخیره کرد.

دسترسی به حساب‌های رایانه‌ای معمولاً با کلمه عبور محرمانه کنترل می‌شود. همانطورکه می‌دانید کلمه عبور اغلب در برابر حدس زدن یا حمله سامانمند برنامه‌هایی که لغاتی از کتاب‌های فرهنگ، اسامی و سایر الگوهای مشترک را امتحان می‌کند آسیب‌پذیر است.

در اصل، کلمه عبور ممکن است با نیروی قدرت‌مآبانه، درست همانند آنچه در مورد کلیدهای رمزی‌سازی می‌دانیم، مورد حمله قرار گیرد. دراین‌صورت برنامه شکننده کلمه عبور، رشته‌های ممکن کاراکترها را ایجاد می‌کند و آنها را در یک برنامه رمزی‌سازی قرار می‌دهد تا کلمه‌ای که کلمه عبور رمزی‌شده را ایجاد می‌کند پیدا شود. بسته به طول کلمه عبور و نوع کاراکترهای مورد استفاده، این کار ممکن است چند ثانیه تا زمانی طولانی وقت بگیرد.

کلمه‌های عبوری ـ که عبارات یا لغات انگلیسی‌اند ـ نسبتاً ضعیف هستند (حتی اگر تا بیست کاراکتر داشته باشند). علت این است که زبان انگلیسی دارای حشویات بسیاری است.

بعضی از ترکیبات حروف (مثلاً The) زیاد تکرار می‌شوند؛ درحالی‌که بسیاری دیگر مانند xgb هرگز وجود ندارد یا به ندرت وجود دارد. بدین‌ترتیب به فرایند جست‌وجو امکان داده می‌شود روی ترکیباتی که احتمال بیشتر دارد تأکید کند. برای جریان طولانی متن، حشویات انگلیسی به حدی است که هر ۲۶ حرف الفبا قابل مقایسه با ۱/۵ تا ۲/۳ بیت است (ولی اگر تمام حروف با احتمال مساوی مورد استفاده قرار می‌گرفت هر ۲۶ حرف، قابل مقایسه با ۴/۷ بیت می‌بود). بنابراین درحالی‌که شکستن یک کلمه عبور ده کاراکتری، درصورتی‌که آن کلمه به‌طور تصادفی از ترکیبات ممکن تمام کاراکترها تشکیل می‌شد، درعمل غیرممکن بود، اگر معلوم شود که کلمه عبور یک عبارت انگلیسی است، شکستن آن نسبتاً آسان است. یکی از کارشناسان امور رمز معتقد است که احتمال شکست موفقیت‌آمیز کلمه عبور، تقریباً پنجاه پنجاه است.

کلمه‌های رمز را می‌توان با انتخاب کلماتی که حداقل هشت کاراکتر طول داشته و در هیچ‌یک از فرهنگ‌های لغات وجود نداشته باشند و حداقل حاوی یک یا دو کاراکتر غیر الفبایی و غیر عددی باشند، در مقابل حملات نسبتاً مصون کرد. بعضی سیستم‌ها کاربران را مجبور می‌کنند کلمه‌های عبوری انتخاب کنند که به‌راحتی قابل شکستن نباشند. این سیستم‌ها با آزمودن کلمه‌های عبور (با یک برنامه شکستن کلمه عبور) در زمان وارد کردن کلمه رمز یا تغییر دادن آن، یا به‌عنوان یک حسابرسی عادی سیستم، کاربر را مجبور به انتخاب کلمه عبوری مناسب می‌کنند. سیستم‌های دیگر برای کاربر به‌طور تصادفی کلمه عبور ایجاد می‌کنند؛ ولی به‌خاطر سپردن این کلمه‌ها مشکل است و کاربر بیشتر تمایل دارد که آن را بنویسد و این امر، آن را در برابر بهره‌برداری آسیب‌پذیر می‌کند. همچنین، کلمه‌های عبوری که به‌طور تصادفی ایجاد شده باشند، اگر ایجادکننده زیاد خوب نباشد، در برابر حمله سامانمند، آسیب‌پذیر هستند. بعضی از سیستم‌عامل‌ها به کلمه عبور «نمک» می‌زنند[1] تا در برابر حملات مبتنی‌بر واژه‌نامه‌ها کمتر آسیب‌پذیر باشند. گفته شد کلمه‌های عبور معمولاً به‌صورت رمزی‌شده در

1. Salting

فایل نگهداری می‌شوند و هریک از آنها به‌عنوان یک کلید، برای رمزی‌سازی بلوک ثابتی از متن ساده (رمزی ساده نشده) به‌کار می‌روند. شکنندگان کلمه عبور، ازطریق گرفتن یکایک لغات یک فرهنگ و به‌کار بردن آن به‌عنوان کلید رمزی‌سازی بلوک ثابت، به‌طور ناگهانی به ورودی فایل حمله، و سپس در فایل کلمه‌های عبور جست‌وجو می‌کنند تا مدخلی را که با آن مطابقت دارد بیابند. با «نمک زدن» به هر کاربر یک نمک منحصربه‌فرد که فقط یک رشته تصادفی از بیت‌های ذخیره‌شده با کلمه عبور متن رمزی‌شده است داده می‌شود. این نمک در طول فرایند رمزی‌سازی مورد استفاده قرار می‌گیرد. کلمه عبور متن رمزی‌سازی‌شده کاربر، هم تابعی از کلمه عبور ساده (رمزی‌سازی نشده) و هم تابعی از نمک است. حال برنامه شکننده کلمه عبور، برای حدس زدن کلمه عبور باید هریک از کلمات فرهنگ لغات را همراه با یکایک نمک‌های ممکن به‌عنوان کلید به‌کار بگیرد که فرایند بسیار وقت‌گیری است.

راه‌حل دیگری که از کلمه عبور ضعیف نیز حمایت می‌کند «کلمه عبور یک‌بارمصرف» است. در این راه‌حل، کلمه عبور کاربر با هر بار ارتباط برقرار کردن، به ترتیبی که در کاربر و سرور ارتباط مشترک است تغییر می‌کند. خود روش می‌تواند علنی و عمومی باشد؛ اما باید به‌نحوی باشد که استراق‌سمع‌کنندگان نتوانند از روی کلمه‌ای که حدس می‌زنند یا سرقت می‌کنند به کلمه موردنظر پی ببرند. کارت شناسایی ایمن[1] که محصول شرکت سکیوریتی داینامیکس[2] است این کار را با ایجاد یک کلمه عبور جدید در هر شصت ثانیه انجام می‌دهد. کلمه عبور، تابعی است از زمان و یک کلید سرّی که مخصوص آن کارت است و سرور هم در آن مشترک است. استفاده از کارت به شماره شناسایی شخصی (PIN) احتیاج دارد و بدین‌ترتیب در برابر سرقت محافظت شده است. روش‌های دیگر ایجاد کلمه عبور یک‌بار مصرف، به ساعت بستگی ندارند؛ ولی تمام آنها به هماهنگ‌سازی[3] بین کاربر و سرور نیازمندند.

1. Secure ID
2. Security Dynamics
3. Synchronization

بعضی از بانک‌ها برای تأمین امنیت در برابر جعل‌کنندگان کارت ماشین‌های خودپرداز از رمزهای یک‌بارمصرف استفاده می‌کنند. هر کارت دارای رمز ایجادشده توسط رایانه است که این رمز با هر بار استفاده از کارت تغییر می‌کند. هر بار معامله تازه‌ای انجام می‌گیرد؛ در بانک به رایانه رمز تازه‌ای تخصیص می‌یابد و بر روی کارت نوشته می‌شود.

۲ـ۳. مجموع بازبیننده‌های یکپارچگی

در بعضی از موقعیت‌ها، جلوگیری از دست‌کاری داده‌ها توسط یک شخص یا برنامه غیرممکن است. یک فرد داخلی (خودی) یا متجاوز ممکن است به فایلی دسترسی غیرمجاز پیدا کند یا ویروس تازه‌ای به سیستم رایانه حمله‌ور شود و فایل‌ها یا بخش بوت[1] را آلوده کند. با توجه به اینکه نمی‌توان مانع دست‌کاری‌های غیرمجاز شد، بهترین رویکرد بعدی کشف آنهاست و این، هدف مجموع بازبیننده‌های یکپارچگی است که در خدمت تأیید اعتبار داده‌ها قرار دارند.

بازبیننده یکپارچگی[2] مقداری است که از روی داده‌های تحت حفاظت محاسبه، و همراه با داده‌ها یا جای دیگر ذخیره می‌شود. یکپارچگی داده‌ها با محاسبه مجدد بازبیننده، کنترل و تأیید می‌شود. اگر حاصل محاسبه جدید با مقداری که ذخیره شده، مطابقت داشته باشد، بدین معنی است که اطلاعات به احتمال زیاد دست‌نخورده باقی مانده‌اند و اگر مطابقت نداشته باشد؛ یعنی اطلاعات دست نخورده نیستند. برای اینکه این کنترل به‌نحو مؤثر عمل کند، مجموع بازبیننده‌ها باید تابعی از یکایک بیت‌های داده‌ها باشد. دراین‌صورت حتی اگر یک بیت تغییر داده شده باشد معلوم می‌شود. به‌علاوه باید چنین باشد که برای هر مجموع بازبیننده معین، پیام دیگری که همان مجموع بازبیننده را نتیجه بدهد وجود نداشته باشد. درغیراین‌صورت نفوذکننده قادر می‌شود پیام صحیح را با پیامی نادرست تعویض کند.

مجموع بازبیننده‌های یکپارچگی را گاهی «رمزهای تأیید اعتبار پیام» یا «اثر انگشت»

---

1. Boot
2. Integrity Checksum

می‌نامند. کاری که تولید مجموع بازبینده می‌کند «عمل تپش‌زنی»[1] می‌نامند؛ زیرا چیزی به‌وجود می‌آورد که شبیه یک بلوک تصادفی داده‌ها از داده‌های اصلی است. مجموع بازبینده، صرف‌نظر از طول پیام، طول ثابتی دارد (طولی بین ۶۴ تا ۱۶۰ بیت).

۲ـ۴. امضاهای دیجیتالی

اختراع رمزی‌نگاری کلید عمومی دو نوآوری تازه به‌همراه آورد. اولین نوآوری، توانایی ارسال پیام به طرف دیگر بدون نیاز به شخص ثالث مورد اعتماد یا کانال خارج خط (خارج رایانه) برای توزیع کلیدی سرّی است. دومین نوآوری، توانایی محاسبه امضاهای دیجیتالی است.

امضای دیجیتالی، بلوکی از داده است که به پیام یا سندی پیوست می‌شود و آن داده را به شخص یا مؤسسه به‌خصوصی منسوب می‌کند. این پیوند به‌نحوی است که امضا می‌تواند توسط دریافت‌کننده یا شخص ثالث مستقل تأیید شود و نمی‌توان آن را جعل کرد. اگر حتی یک بیت از داده حذف شده باشد، امضا در فرایند تأمین اعتبار رد می‌شود. امضاهای دیجیتالی، اعتبار منبع یک پیام را نشان می‌دهد. به‌علاوه، امکان انکار را ازبین می‌برد؛ زیرا کسی نمی‌تواند منکر امضا کردن پیام شود و خود را وارهاند. غیر از مواردی که کلید خصوصی شخص مورد بهره‌برداری قرار گرفته است کسی نمی‌تواند آن امضا را به‌وجود آورد.

معمولاً امضای دیجیتالی ثابت نمی‌کند که سند توسط امضاکننده نوشته شده، فقط ثابت می‌کند که امضاکننده به آن دسترسی داشته و آن را امضا کرده است. سند ممکن است دزدیده شده باشد؛ ولی در اوضاع و احوالی که فرایند امضا با ایجاد سند همراه است، امضا یک گواه منطقی در مورد اصل بودن سند است. دوربین‌های دیجیتالی نمونه‌ای مناسب از این امر را ارائه می‌دهند. اگر یک دوربین دیجیتالی به‌منظور امضا کردن عکس در زمان گرفتن آن دارای یک کلید خصوصی باشد، امضا دلیل محکمی به این واقعیت است که عکس توسط آن دوربین

1. Hashing

گرفته شده است. این امر می‌تواند در برابر دست‌کاری رایانه‌ای در تصویر دیجیتالی که کار نسبتاً ساده‌ای است محافظت ایجاد نماید. عکس‌های امضاشده به‌ویژه می‌توانند در محاکمات جنایی سودمند باشند؛ زیرا متهم سعی می‌کند مدعی شود که عکس اثبات‌کننده، ساختگی است. دوربین‌های ویدئویی، گیرنده‌های صوتی و سایر دریافتگرها (سنسورها) نیز می‌توانند برای اثبات اصل بودن خروجی، خروجی‌های خود را امضا کنند.

امضای دیجیتالی می‌تواند در کاربردهایی که در آنها تأمین اعتبار موردنظر است، ولی نیازی به سرّی بودن نیست، بدون رمزی‌سازی پیام مورد استفاده قرار گیرد.

برای امضای تأیید اعتباری در رایانه‌ها، استفاده از ماشین‌های خودپرداز بانک‌ها و ورود به تأسیسات نیز می‌توان از امضاهای دیجیتالی استفاده کرد. در این روش، کلید خصوصی باید در نوعی کارت ذخیره، و در خلال تأیید اعتبار وارد دستگاه قرائت شود. دستگاه تأیید اعتبار، چالشی را که دارای امضای خصوصی شخصی خواهد بود صادر می‌کند. دستگاه درحین استفاده از کلید عمومی مربوطه، اعتبار چالش امضاشده را کنترل و تأیید خواهد کرد.

برخلاف کلیدهای مورد استفاده در رمزی‌سازی (محافظت از محرمانه بودن)، کلیدهای خصوصی مورد استفاده برای امضا کردن پیام‌ها معمولاً به‌منظور بازیافت کلید بایگانی نمی‌شود. بازیافت این کلیدها مطرح نیست؛ زیرا امضاها با کلیدهای عمومی که می‌توانند به‌طور وسیع بخش شود تصدیق شده‌اند. اگر کلید خصوصی یک امضا گم شود، می‌توان یک کلید نو ساخت و کلید عمومی قدیمی را منقضی کرد (هنوز از آن می‌توان برای تأیید اعتبار اسنادی که قبلاً امضا شده‌اند استفاده کرد). به‌علاوه اگر کلیدهای امضای خصوصی در دست یک شخص ثالث باشد، آنها مقداری از ارزش خود را در تأیید اعتبار کاربر و مدارک و شواهد پرونده‌های کیفری از دست خواهند داد؛ زیرا عامل بازیافت می‌تواند از کلیدهای ذخیره‌شده برای جعل امضای صاحبان آنها استفاده کند.

رمزی‌نگاری کلید عمومی در ابتدا برای حل کردن مشکل مدیریت کلید، یعنی توزیع کلیدهای پیام سرّی اختراع شد؛ ولی با این عمل، مشکل دیگر مدیریت کلید که توزیع و

استفاده از کلیدهای عمومی نادرست یا مورد بهره‌برداری قرار گرفته، خود را نشان می‌دهد.

سوابق دیجیتالی موسوم به «گواهی‌های کلید عمومی» به تهدید کلیدهای عمومی جعلی می‌پردازد. این سوابق که توسط یک «مقام گواهی‌کننده» ایجاد و امضا می‌شود، در اصل درستی یک کلید عمومی و شاید قابلیت اعتماد صاحب آن را تصدیق می‌کند. هر گواهی دیجیتالی حاوی یک کلید عمومی، یک شناساننده منحصربه‌فرد مخصوص سوژه صاحب کلید و امضای مقام گواهی‌کننده است. بیشتر گواهی‌ها مطابق نسخه ۳ استاندارد ANSIX 509 است که به X.509v3 نشان داده می‌شود. این استاندارد حاوی میدان‌هایی برای الگوریتم کلید عمومی که با کلید مورد استفاده قرار می‌گیرد، مدت اعتبار کلید، نام صادرکننده و شناسایی منحصربه‌فرد و چیزهای دیگر است.

۲ـ۵. بوم نقش‌ها

بوم نقش، الگوی مشخصی است که توسط مبدأ داده‌ها در یک سند، تصویر یا شیء صوتی منقوش می‌شود. بوم نقش می‌تواند در خدمت چندین منظور مختلف مانند: تثبیت مالکیت بر داده‌ها، پیگیری نسخه‌های داده‌ها و تأیید یکپارچگی داده‌ها باشد؛ برای مثال، بوم نقش در اسکناس دلیل این است که پول در چاپخانه مورد تأیید به چاپ رسیده است. بوم نقش ممکن است با چشم غیرمسلح قابل رؤیت نباشد (یا گوش نتواند آن را بشنود)؛ اما برای دیدن (یا شنیدن) آن به‌منظور اثبات اعتبار داده‌ها یا منبع آن باید وسیله‌ای وجود داشته باشد.

داده‌های دارای بوم نقش تابع شناساننده یا کلیدی هستند که مختص خود مبدأ (به‌وجود آورنده) است. ممکن است برای کشف یا استخراج بوم نقش، این شناساننده‌ها یا کلیدها مورد نیاز باشند. اگر چند نسخه اطلاعات منبع، بوم نقش جداگانه داشته باشند، هرکدام را می‌توان با کلیدی جداگانه پردازش کرد؛ یعنی هر نسخه، «اثر انگشت» خاص خود را دارد. صاحب داده‌ها با پی بردن به اینکه کدام کلید مورد استفاده کدام مشتری قرار گرفته، می‌تواند منبع نقض حقوق انحصاری ثبت‌شده را مشخص کند.

بوم نقش ممکن است شکننده یا قوی باشد. نوع شکننده آن که به آسانی فاسد می‌شود، برای تعیین اینکه در داده‌ها تغییری داده شده یا نه، سودمند است. بوم نقش‌های قوی نیز در برابر دست‌کاری و حذف، مقاومت می‌کنند و برای تعیین مالکیت و ردیابی نسخه‌هایی که از آنها استفاده نادرست شده باشد، مناسب‌ترند.

فرایند بوم نقش‌سازی مشابه فرایند سرّی‌سازی است و از تکنیک‌های آن پیروی می‌کند؛ مثلاً یک روش بوم نقش‌سازی که به داده‌های دیجیتالی مربوط می‌شود، گنجاندن یک سند هویت و کلید در داخل صدا، تصویر و فایل ویدیویی است. اگر سند هویت و کلید، شناخته شده باشند، تعیین اینکه در داده‌ها وجود دارند یا ندارند آسان است.

۲ـ۶. تلفن به تلفن‌کننده و تلفن به خانه

سازوکار تلفن به تلفن‌کننده می‌تواند به دفاع در برابر کسانی که با تلفن، خود را شخص دیگری معرفی می‌کنند کمک کند. وقتی کسی به «ارتباط تلفنی» زنگ می‌زند، سیستم نام شخص را سؤال می‌کند. سپس شماره تلفن اشخاصی را که در بانک اطلاعاتی داخلی خود (حاوی نام اشخاص معتبر) دارد جست‌وجو کرده، به تلفن‌کننده زنگ می‌زند و فرایند را تکمیل می‌نماید. بدین‌ترتیب حتی اگر شخص متجاوز به‌نحوی نام حساب و کلمه عبور شخصی را به‌دست آورده باشد، قادر به ورود نخواهد شد؛ زیرا تلفن برگشت، شماره کاربر را می‌گیرد نه شماره متجاوز را. ولی این سیستم خالی از ضعف نیست. متجاوز ممکن است به‌طور غیرمجاز وارد سیستم تلفن شود و تلفن به کاربر را به تلفن به خود هدایت کند.

مؤسسات تجاری برای تأیید سفارش‌های تلفنی، به‌نوعی اینگونه رفتار می‌کنند؛ برای مثال، رستورانی که به سفارش مشتری، غذا را در محل مورد تقاضای او تحویل می‌دهد، پس از دریافت سفارش پیتزا، برای تأیید سفارش به مشتری تلفن می‌کند. این اقدام مانع آن می‌شود که شوخ‌طبعان، به نام هدف‌های خود غذا سفارش بدهند. در اینترنت گاهی برای تأیید اعتبار سفارش‌های خرید یا تقاضاهای قرار گرفتن در لیست توزیع، از روش مشابهی استفاده می‌شود.

دراین‌حالت بازرگان یا مدیر لیست به کاربری که تقاضای تأیید کرده، با پست الکترونیک پیام ارسال می‌کند. این اقدام در برابر دزدان هویت که به حساب قربانیان خود کالا سفارش داده یا نام قربانیان خود را در صدها لیست توزیع پیام پست الکترونیکی قرار می‌دهند تا سیل پیام‌های الکترونیکی به سوی آنها جاری شود ایجاد حفاظت می‌کند.

در نوع دیگری از این وسایل، صاحب رایانه کیفی[1] می‌تواند نرم‌افزاری نصب کند که به ایستگاه کنترل مرکزی، تلفن نموده، شناسانندهٔ الکترونیکی خاصی را به آن ایستگاه مخابره می‌کند. ایستگاه کنترل با استفاده از سند هویت تلفن‌کننده بررسی می‌کند که تلفن از همان شماره‌ای که به آن سند هویت تعلق دارد صورت گرفته یا نه. اگر از همان شماره تلفن نبود، می‌تواند نشانه آن باشد که رایانه کیفی دزدیده شده است.

۲ـ۷. تأیید اعتبار مبتنی‌بر محل

مشخصه فضای رایانه‌ای اغلب دنیای مجازی است که مافوق فضا قرار دارد. افراد وارد رایانه می‌شوند و بدون توجه به موقعیت جغرافیایی خود و محل سیستم‌های مورد استفاده، تجارت الکترونیکی انجام می‌دهند. یک پیامد این امر آن است که اقدامات می‌تواند در مودم‌ها و شبکه‌های رایانه‌ای انجام گیرد، بی‌آنکه کسی به‌طور دقیق بداند مبدأ آنها کجاست. پیدا کردن کسی که مرتکب تجاوز رایانه‌ای شده یا جرمی در فضای رایانه انجام داده، فوق‌العاده دشوار و اغلب غیرممکن است (به‌ویژه اگر مرتکب، از رایانه‌های متعددی در جهان گذشته و به هدف رسیده باشد).

تأیید اعتبار مبتنی‌بر محل، روشی برای تأیید اعتبار مؤسسه در فضای رایانه، براساس موقعیت ژئودزیک[2] (طول جغرافیایی، عرض جغرافیایی و ارتفاع در یک سیستم مرجعِ هماهنگِ زمین مرکزی که به دقت تعریف شده) است. اثر آن به زمین آوردن فضای رایانه‌ای

1. Laptop
2. Geodesic

(به دنیای فیزیکی آوردن آن) است؛ به‌نحوی‌که موقعیت فیزیکی کاربران (و متجاوزان) را بتوان به‌نحو قابل اطمینانی تعیین کرد. با کنترل‌های مبتنی‌بر محل، دیگر واردشونده غیرمجاز به سیستم‌های رایانه‌ای که ساکن روسیه است نمی‌تواند وارد سیستم انتقال پول در انگلستان شود و وانمود کند که از بانکی در آرژانتین تماس می‌گیرد.

تأیید اعتبار مبتنی‌بر محل، برای محافظت از سایت‌های ثابت به بهترین وجه مؤثر است؛ زیرا دریافتگر را می‌توان بالای سقف یا پنجره که دید خوبی در آسمان دارد قرار داد. چون سیگنال‌های GPS از دیوار و سقف عبور نمی‌کنند، این فناوری را نمی‌توان در همه‌جا مورد استفاده قرار داد؛ برای مثال با اینکه دریافتگر خیلی کوچک است، نمی‌توان آن را به رایانه کیفی نصب کرد یا روی میز و اتاق هتل مورد استفاده قرار داد؛ بنابراین برای تأمین اعتبار کاربران سیار، مناسب نیست (البته سرانجام بر محدودیت‌های این فناوری غلبه خواهد شد). اینکه این فناوری برای سایت‌های ثابت مناسب‌تر است، دلیل دیگری نیز دارد و آن این است که این سیستم، اعتبار محل دریافتگر امضای محل (LSS)[1] را تعیین می‌کند نه اعتبار کاربر را. کاربر می‌تواند در محدوده‌ای که می‌تواند با دریافتگرهای امضای محل ارتباط سریع پیدا کند در همه‌جا باشد. اگر محل دریافتگر امضای محل، به‌طور فیزیکی مورد حفاظت باشد، متجاوزان خارجی قادر نخواهند بود برای برقراری ارتباط با آن با نصب دریافتگر امضای محل خود به‌جای دریافتگر امضای محل اصلی، به آن دسترسی پیدا کنند.

از تأیید اعتبار محل می‌توان به‌عنوان محضردار الکترونیکی هم استفاده کرد. دفتردار می‌تواند یک امضای محل به یک سند اضافه کند و بدین‌ترتیب تصدیق نماید که آن سند در فلان لحظه و فلان محل وجود داشته است. محضردار می‌تواند برای محافظت سند در برابر جعل، تمام بسته را امضای دیجیتالی کند. این اسناد محضری می‌تواند در حل اختلافات مربوط به حق ثبت و سایر اختلافات مالکیت معنوی مورد استفاده قرار گیرد.

1. Location Signature Sensor

یکی از معایب تأیید اعتبار محل این است که اگر سیگنال «سیستم موقعیت‌یاب جهانی»[1] دستخوش پارازیت شود یا «دریافتگر امضای محل» به سرقت برود، ممکن است در برابر حمله ممانعت از سرویس، آسیب‌پذیر باشد.

عیب دیگرش این است که فناوری مزبور به‌طور بالقوه می‌تواند به‌عنوان یک سلاح نبرد اطلاعاتی تهاجمی، برای ردیابی محل فیزیکی افراد مورد استفاده قرار گیرد. برای حفظ منافع خصوصی مشروع افراد می‌توان دسترسی به آن نوع اطلاعات ژئودزیک را که به‌منظورهای معین (مانند تأیید اعتبار برای ورود به سیستم) جمع‌آوری شده، به‌شدت محدود نمود. درواقع هم‌اکنون نیز قوانین موجود، دسترسی دولت به این نوع اطلاعات را کنترل کرده است. بخش خصوصی دسترسی را می‌توان با قرارداد و انواع موافقت‌نامه‌های تجاری و درصورت لزوم، مقررات دیگر تحت کنترل درآورد. می‌توان فقط اطلاعاتی را که برای کاربردی خاص لازم است مورد استفاده قرار داد و نگهداری کرد و بدین‌ترتیب به حریم خصوصی افراد احترام گذاشت. سومین تضمین این است که به کاربران تا حدی امکان داده شود بر انتشار محل ژئودزیک خود کنترل داشته باشند (شبیه توانایی برای «خارج کردن خود» و «مسدود کردن» سند هویت تلفن‌کننده). این نوع مسدود کردن، شخص را در برابر سوءاستفاده کسانی که نیازی به آن نوع اطلاعات ندارند محافظت می‌کند. اعلام محل ژئودزیک می‌تواند داوطلبانه، ولی درعین‌حال بدون ارائه محل ژئودزیک بعضی اقدامات (مانند دسترسی به یک معامله یا سیستم خاص) ممنوع باشد.

در خصوص پلاک‌ها و کارت‌ها بسیاری از انواع تأیید اعتبار می‌تواند همراه با کارت پلاستیکی یا انواع دیگر کارت‌هایی که برای کنترل دسترسی به ساختمان‌ها و اتاق‌ها، رایانه‌ها، حساب‌های بانکی و سایر منابع اطلاعات مورد استفاده قرار می‌گیرد انجام شود. در این کارت‌ها می‌توان علاوه‌بر کلیدهای امضای دیجیتالی و داده‌های زیست‌سنجی، اطلاعات دیگر مربوط به دارنده کارت یا کاربر آن (مانند: نام، نشانی، شماره حساب بانکی، شماره کارت

---

1. Global Positioning System (GPS)

اعتباری، اطلاعات پزشکی، حق دسترسی و غیره) را نیز ذکر کرد. این اطلاعات را می‌توان با رمزهای خطی، خط‌های مغناطیسی و تراشه‌های ریزپردازنده رمزی کرد. بعضی از کارت‌ها دارای عکس هستند. عکس را می‌توان با دوربین گرفت و به کارت الصاق کرد و بعد برای زیادتر کردن دوامش، آن را ورقه‌ورقه نمود. فناوری تصویری جدید، این امکان را نیز به‌وجود آورده است که عکس، به‌طورمستقیم روی کارت چاپ شود.

فناوری دیگر، کارت‌هایی است که خودبه‌خود پس از انقضای مدت اعتبار باطل می‌شوند. این کارت‌ها با کاغذ حرارتی حساسی در برابر نور ساخته یا با جوهر مخصوصی که پس از سپری شدن مدت زمان معین ... آن می‌پرد نوشته می‌شوند و به‌عنوان پلاک‌های موقت مخصوص بازدیدکنندگان وسیله خوبی هستند. بازدیدکننده‌ای که ساختمان را ترک می‌کند و پلاک را با خود می‌برد، برای بار دوم نمی‌تواند از آن استفاده کند و وارد ساختمان شود.

۴. امنیت اطلاعات و تضمین اطلاعاتی

عبارت «امنیت اطلاعات»[1] حداقل دو یا سه دهه است که به‌کار می‌رود. یکی از استانداردهای دولت فدرال ایالات متحده، امنیت اطلاعات را چنین تعریف می‌کند «محافظت از اطلاعات در برابر افشای غیرمجاز، انتقال، تغییر یا انهدام به‌طور تصادفی یا عمدی».[2] برعکس عبارت مذکور، عبارت «تضمین اطلاعاتی» نسبتاً جدید است. در رهنمود ۱۹۹۶ وزارت دفاع ایالات متحده، تضمین اطلاعاتی چنین تعریف شده است «عملیات اطلاعاتی که اطلاعات و سیستم‌های اطلاعات را ازطریق تضمین موجود بودن، تمامیت، اعتبار محرمانه ماندن و عدم مغایرت، محافظت و از آنها دفاع می‌کند. احیای سیستم‌های اطلاعاتی ازطریق ادغام قابلیت‌های محافظت، کشف و واکنش ازجمله این عملیات است».[3]

---

1. Info Sec
2. Erik Kirschbaum, **Reuters**, Bonn, Nov. 17, 1997.
3. John Diamond, "CIA Seeks to Provide Warnings of Global Conflicts", **Assodated Press**, Dec. 27, 1997.

نبرد اطلاعاتی دفاعی با هر دوی این مفاهیم رابطه نزدیک دارد؛ ولی فقط به حملات عمدی می‌پردازد. امنیت اطلاعات و تضمین اطلاعاتی، حملات غیرعمدی مانند: خطاها (خطاهای سخت‌افزاری، نرم‌افزاری و انسانی)، تصادفات و بلایای طبیعی را نیز درنظر می‌گیرد. پاره‌ای از پرهزینه‌ترین تهدیدات دارای ماهیت غیرعمدی هستند. دراین‌خصوص، مشکل «سال ۲۰۰۰» مثال خوبی[1] است. هزینه‌هایی که در سطح جهان برای این معضل انجام می‌گیرد بسیار زیاد است. عده‌ای این هزینه را میلیاردها دلار یا بیشتر برآورد کرده‌اند. عدم توجه کافی به این مشکل می‌تواند به زیان‌های عظیمی که ناشی از اقدام واردشوندگان غیرمجاز به رایانه‌ها در برابر آن هیچ است منجر شود. لذا با اینکه مشکل سال ۲۰۰۰ به‌خودی‌خود اقدام نبرد اطلاعاتی نبود، می‌تواند مورد بهره‌برداری رزمندگان نبرد اطلاعاتی قرار گیرد. بروس برکوویتز[2] هشدار می‌دهد که طرفین متخاصم ممکن است از تلاش‌های فراوانی که برای اجیر کردن برنامه‌نویسان برای تعمیر سیستم‌ها انجام می‌شود بهره‌برداری کنند. آنها می‌توانند با استفاده از این فرصت، تکنسین‌هایی را به‌صورت نفوذی وارد شرکت‌ها، مؤسسات، سازمان‌های مالی و خدمات حمل‌ونقل نمایند. این عوامل نفوذی، وقتی جزء داخلی‌ها شدند می‌توانند ویروس، بمب‌های منطقی و راه‌های پنهان نفوذ برای استفاده‌های آتی را در آن سازمان‌ها کار بگذارند.[3]

هم نبرد اطلاعاتی دفاعی و هم تضمین اطلاعاتی، به تهدیداتی که در قلمروی امنیت اطلاعات قرار ندارند (ازجمله: عملیاتی مانند مدیریت درک که در آن از رسانه‌های جمعی بهره‌برداری می‌شود) می‌پردازند. پیامدهای هدف قرار گرفتن به‌منظور ایجاد شهرت بد یا بدنام

---

۱. این مشکل از آنجا ناشی می‌شد که طراحان نرم‌افزارهای کامپیوتری، هنگام ثبت تاریخ تنها دو رقم سمت چپ را درنظر گرفته بودند و ورود به سال ۲۰۰۰ بسیاری از سازمان‌ها، نهادها و کشورها را با مشکل مواجه ساخت. تخمین زده شده است که در حدود ۴۰۰ میلیارد دلار هزینه برای گذر از این خطا، صرف شد.

2. Bruce Berkowitz

3. Bruce Kammer, "Information Warfare: The Revolution in Military Affairs and How the US Is Adapting to the Future of Warfare", **Term paper for COSC 511, Georgetown University**, May 1, 1997, Citing Norman Friedman, "Desert Victory: The War for Kuwait", **United States Naval Institute Press**, Annapolis, MD, 1991, pp. 172-178.

کردن، معمولاً بخشی از امنیت اطلاعاتی که بیشتر با محافظت از منابع اطلاعات متعلقه یا تحت مدیریت سروکار دارد نیست؛ ولی مدیریت درک می‌تواند به اندازه واردشوندگان رایانه‌ها (اگر نگوییم بیش از آنها) در وضع رقابتی سازمان یا فرد تأثیر بگذارد. درواقع یکی از دلایل اینکه شرکت‌ها موارد تجاوز به رایانه‌های خود را گزارش نمی‌کنند همین است. آنها بیم دارند با خطر ازدست دادن اعتماد عمومی مواجه شوند. سازمان‌ها درنوع خود به این تهدیدات رسانه‌های همگانی می‌پردازند؛ ولی ازطریق ادارات روابط عمومی خود نه ازطریق ادارات امنیت اطلاعات.

۳ـ۱. مدل سی‌آی‌ا و اعتبار

امنیت اطلاعاتی را اغلب به سه عنصر اصلی تقسیم می‌کنند که عبارتند از: محرمانگی،[1] تمامیت[2] و موجود بودن.[3] گاهی سی‌آی‌ا امنیت اطلاعات نامیده می‌شود؛ زیرا حروف اول سه عنصر فوق، به زبان انگلیسی است. محرمانگی یعنی اینکه اطلاعات فقط در زمان‌های مجاز و به روش مصوب در اختیار مؤسسات مجاز قرار بگیرد و برای آنها فاش شود. در مدل نبرد اطلاعاتی، محرمانگی با مفهوم موجود بودن آن برای حمله درنظر گرفته شده است. هدف از دفاع، مغلوب کردن حملاتی است که به‌منظور افزایش در دسترس بودن آن اطلاعات انجام می‌گیرد. در هر دو مدل، تمامیت یکی است و شامل اعتبار و بدنام نشدن می‌شود. هدف دفاع، محافظت در برابر کاهش تمامیت است. بالاخره، موجود بودن در مدل امنیت اطلاعات معادل موجود بودن برای دفاع در مدل نبرد اطلاعاتی است. در اینجا، هدف عبارت است از: دفاع در برابر حملاتی که می‌کوشد این موجود بودن را کاهش دهد.

مدل نبرد اطلاعاتی مدل استاندارد CIA را به دو مفهوم موجود بودن و تمامیت تقلیل

1. Confidentiality
2. Integrity
3. Availability

می‌دهد؛ اما بین موجود بودن برای حمله و موجود بودن برای دفاع تفاوت قائل می‌شود. مدل نبرد اطلاعاتی، با این عمل مفهوم متقارن موجود بودن برای دفاع و حمله را می‌پذیرد. به‌علاوه، مفهوم موجود بودن برای حمله، دامنه‌ای گسترده‌تر از تهدیداتی که فقط در محرمانگی مدنظر است دارد و تجاوز به حق طبع یا تألیف را که بیشتر به مفهوم انحصاری بودن نزدیک است تا محرمانگی نیز دربرمی‌گیرد. دسترسی غیرمجاز به رایانه‌ها و سیستم تلفن، صرف‌نظر از اینکه داده‌های حساس در معرض قرار می‌گیرند یا نه، نیز در این مقوله قرار دارد. برقراری کنترل بر رسانه‌های همگانی نیز مشمول آن است. مدل CIA بر اصل مجوز (چه کسی اجازه دسترسی به چه چیز را دارد و با کدام روش) استوار است. در این اصل «چه کسی» می‌تواند هر موجودیتی باشد که قادر به عمل است و شامل اشخاص و نرم‌افزارهای رایانه‌ای نیز می‌شود. «چه چیز» می‌تواند هر منبع اطلاعاتی در هرکدام از رسانه‌ها و شامل: اسناد چاپی، دیسکت‌ها و نوارها، مخابرات نقطه‌به‌نقطه، برنامه‌های پخش‌شده رادیو و تلویزیون و رایانه‌ها و شبکه‌های رایانه‌ای باشد. منظور از «دسترسی به کدام روش» کاری است که بازیگر اجازه دارد با منبع اطلاعات انجام دهد. آیا بازیگر اجازه استفاده از آن را دارد؟ اجازه تماشا کردن چطور؟ اجازه دارد آن را تغییر دهد، توزیع کند یا ازبین ببرد؟ آنچه بازیگر می‌تواند با یک منبع انجام دهد، به نوع رسانه بستگی دارد؛ برای مثال، عملیاتی که به رسانه‌های چاپی مربوط می‌شوند عبارتند از: تماشا کردن، تغییر دادن، ازبین بردن، رونوشت برداشتن (کپی تهیه کردن) و توزیع. امنیت اطلاعات با دفاع در برابر اقدامات غیرمجاز بدون ممنوع کردن اقدامات مجاز سروکار دارد. به‌طور خلاصه «بگذار بدها خارج شوند و درعین‌حال خوب‌ها وارد گردند».

خط‌مشی‌های مربوط به این اجازه‌ها می‌تواند تابع قرارداد، مقررات یا قانون باشد و به‌وسیله کسانی که صاحب آن منابع اطلاعات هستند یا آنها را در کنترل دارند، به‌طور رسمی یا غیررسمی تعیین شود؛ مثلاً اقداماتی که می‌توان در مورد مالکیت معنوی (حقوق ثبت‌شده، حق طبع، علائم تجاری و اسرار تجاری) انجام داد، تابع قانون مالکیت معنوی و قراردادهای عدم افشا و لیسانس است.

سازمان‌های بسیاری برای برچسب زدن به اطلاعات حساس دارای طرح‌های طبقه‌بندی هستند؛ برای مثال، مؤسسه‌ای ممکن است به اطلاعات برچسب «همگانی»، «محرمانه» و «مصرف داخلی» بزند. این برچسب‌ها در داخل شرکت محدودیت‌های دسترسی و سروکار داشتن با اطلاعات را مشخص می‌کنند. همچنین ممکن است اطلاعات را برحسب پروژه یا گروه کاری به‌صورت مجموعه‌های جداگانه درآورند. بدین‌ترتیب اطلاعاتی که به پروژه‌ای مربوط است، برای پروژه‌های دیگر غیرقابل دسترسی است.

در ایالات متحده اطلاعات دولتی که برای امنیت ملی حساس و مهم دانسته می‌شوند به موجب قانون تنظیم شده، تابع یک سیستم طبقه‌بندی و اجازه هستند. سه سطح طبقه‌بندی اساسی وجود دارد که عبارتند از: خیلی سری، سری و محرمانه. اطلاعاتی که افشای غیرمجاز آنها به‌طور منطقی می‌تواند موجب وارد آمدن خسارت وخیم و استثنایی به امنیت ملی گردد، با «خیلی سری» مشخص می‌شوند. «سری» اطلاعاتی است که می‌توان به‌طور منطقی انتظار داشت افشای غیرمجاز آنها موجب وارد آمدن خسارت جدی به امنیت ملی گردد و «محرمانه» یعنی اطلاعاتی که می‌توان به‌طور منطقی انتظار داشت افشای غیرمجاز آنها موجب وارد آمدن خسارت به امنیت ملی گردد.

برای اینکه فردی به اطلاعات متعلق به یکی از این طبقات دسترسی پیدا کند، به اجازه‌ای در آن سطح یا سطح بالاتر نیاز دارد. این فرایندی است که در آن، کنترل زمینه‌ها وجود دارد. به‌علاوه شخص باید به دانستن آن اطلاعات نیازمند باشد. اطلاعات فوق‌العاده حساس، مورد تقسیم‌بندی به‌صورت مجموعه‌های جداگانه نیز قرار می‌گیرند که دراین‌صورت برای دسترسی پیدا کردن به آنها اجازه‌های دیگری نیز لازم است. بالاخره اینکه می‌توان به اطلاعات، علامت‌هایی مانند «هیچ تبعه خارجی» نیز زد. افشای غیرمجاز اطلاعات طبقه‌بندی‌شده می‌تواند جرم مشمول قوانین باشد. سیستم‌های طبقه‌بندی دولتی می‌تواند اطلاعات را از دست رهبران حکومت و نیز مردم دور نگاه دارد.

مفهوم مجوز را می‌توان به نبرد اطلاعاتی دفاعی نیز بسط داد؛ اما با یک محدودیت. در

مورد منابع غیرمتعلق به خود، اگر هر قدرت بالا اجازه دسترسی بـه آن منـابع را داشـته باشـد، دفاع می‌تواند کم باشد، نبرد اطلاعاتی دفاعی باید به منابع غیرمتعلق به خود، به‌ویژه منـابع بـاز رسانه‌ای مانند: رادیو، تلویزیون و روزنامه‌ها نیز توجه نماید.

اغلب گفته می‌شود تنها راه ایمن نگاه داشتن سیستم رایانه‌ای این است کـه پریـز آن را از بـرق بکشیم. البته این عملی نیست؛ اما مشکل بودن حفظ منابع اطلاعات از حملات هماهنگ را بـه ذهن متبادر می‌کند. هرچه دسترسی کمتر باشـد، امنیـت بیـشتر اسـت. درواقـع هـدف امنیـت اطلاعات، بسیار جالب‌تر و چالش‌برانگیزتر است. هدف، منع دسترسی (که خود، نـوعی حملـه است) نیست، بلکه فقط منع دسترسی غیرمجاز، آن هم با اقتصادی‌ترین و نامـشهودترین روش ممکن است. قصد این است که امنیت اطلاعات از مأموریت یک سازمان پشتیبانی کنـد و ایـن پشتیبانی به دسترسی به‌موقع به منابع اطلاعات بستگی دارد.

فصل ششم

عرصه نبرد الکترونیکی و نبرد اطلاعاتی

- درآمد
- جنگ الکترونیک

۱. درآمد[1]

جنگ حرفه‌ای پیچیده است و ظهور عصر الکترونیک روند امور را چندان ساده نکرده است. در دهه‌های پس از جنگ جهانی دوم، مفهومی تحت عنوان «فرماندهی، کنترل، ارتباطات و اطلاعات»[2] تکوین یافت و بدان معنا بود که چنانچه فرماندهی حجم کافی ارتباطات و اطلاعات را ـ که به‌صورت الکترونیکی در اختیارش قرار داده می‌شود ـ در دست داشته باشد می‌تواند با کارایی قابل ملاحظه‌ای با واحدهای تابعه خویش به‌صورت الکترونیکی ارتباط برقرار نماید. نظریه مزبور در خلال قسمت اعظم قرن بیستم به‌خوبی جامه عمل نپوشید و استفاده اولیه از ارتباطات الکترونیکی نظامی تنها در چارچوب بهره‌گیری از منابع تلگراف غیرنظامی موجود بود. ارتش‌ها برای مهیا ساختن سیستم‌های نظامی‌شده هیچ تلاشی نکردند. جنگ جهانی اول نیز تا حد زیادی نوعی وضعیت آشفته بود. با آغاز جنگ جهانی دوم سیستم‌های نظامی معمول بیشتری به‌ویژه در زمینه کنترل توپخانه و هواپیماها به‌وجود آمد. هر دو سیستم مزبور نیازمند آن بودند که پیش‌ازآنکه در صحنه نبرد به‌کار گرفته شوند، تا حد قابل ملاحظه‌ای مورد تجدید نظر قرار گیرند و عیب‌زدایی گردند.

درحال‌حاضر جدیدترین سیستم‌ها نیز سه مشکل عمده دارند:

---

۱. این متن اقتباسی است از فصل هجدهم کتاب ذیل:

James F. Dunnigan, **How to Make War: A Comprehensive Guide to Modern Warfare in Twenty-First Century**, 4th ed., New York: HarperCollins Publishers, 2003.

2. Command, Control, Communications and Intelligence (C3I)

- پیچیده هستند و با افزوده شدن ویژگی‌های جدید و ترمیم ویژگی‌های موجود، به‌طور مداوم تغییر مداوم می‌یابند.
- فرماندهان و کارکنانی که از سیستم‌های مزبور استفاده می‌کنند، تجربه استفاده از آنها به‌ویژه تحت شرایط آشفته و نامعین جنگ را ندارند. قسمت اعظم سیستم‌های مزبور به‌صورت تصادفی در جنگ نابود می‌شوند. مشکلات فنی غیرمترقبه‌ای رخ خواهد داد و نتایج مشکلات مزبور و راه‌حل آنها تا زمان تهاجم جنگ مشخص نخواهد شد.
- با مشاهده وضعیت نمایش داده‌شده روی صفحه رایانه، نوعی امنیت کاذب حاصل می‌آید. جهان واقع اینگونه نیست و کاربران باید بیاموزند چگونه نسخه الکترونیکی نبرد را با آنچه واقعاً رخ می‌دهد مرتبط نمایند.

هنگامی که فرماندهان می‌کوشیدند با تمامی ابزارهای فرماندهی، کنترل، ارتباطات و اطلاعات مزبور جنگی را اداره نمایند، برای آنکه درخصوص آنچه رخ می‌داد نگران باشند، توجیه خوبی داشتند. این مسئله در جنگ خلیج‌فارس در سال ۱۹۹۱ رخ داد؛ هنگامی‌که هواپیماهای جی استارز[1] ایالات متحده آخرین حلقه زنجیره کنترل الکترونیکی را که بیش از یک قرن ایجاد آن به طول انجامیده بود تکمیل کرد. برای اولین‌بار در تاریخ، فرماندهان شاهد آن بودند که واحدها به‌طور همزمان در محدوده‌ای با صدها کیلومتر مربع مساحت حرکت می‌کنند. مشکل این بود که تصاویر روی صفحه‌های رایانه به‌درستی تشخیص نمی‌دادند که این واحدها کدامیک هستند. لحظات نگران‌کننده‌ای نیز وجود داشت که گردان‌های آمریکایی و انگلیسی با آتش دشمن روبه‌رو گردند. این مسئله پیش‌ازاین نیز اتفاق افتاده بود؛ اما مکالمات رادیویی نشان می‌داد که نیروها خودی هستند یا خیر، و مانع از آن می‌شد که حادثه معمول جنگ‌های قرن بیستم، یعنی گشودن آتش به روی نیروهای خودی تکرار گردد.

نیروهای مسلح ایالات متحده با درک این مسئله کل دهه نود را به فعالیت برای حل این

---

1. JSTARS

مشکل اختصاص دادند. راه‌حل آنان «دیجیتالی شدن» بود. ظهور شبکه جهانی در اواسط دهه نود می‌توانست دراین‌خصوص کاری انجام دهد. ایده کلی نوعی شبکه میان نیروهای خودی در صحنه نبرد بود؛ اما تلاشی دیگر برای کارکرد بهتر فناوری اطلاعات در این صحنه نیز محسوب می‌شد. استفاده از «دیجیتالی شدن» در صحنه نبرد به‌معنای قرار دادن نمایشگرهای رایانه‌ای در اغلب وسایل نقلیه فرماندهی و جنگی بود. برهمین‌اساس اطلاعات درخصوص محل استقرار سربازان خودی و دشمن و نیز موقعیت اشیایی چون: میدان‌های مین و موانع در نمایشگرهای خودروها قابل رویت بود. ازآنجاکه این نمایشگرها از نظام نمادها استفاده می‌کنند، سربازان می‌دانند که هرچیز در کجا قرار دارد و بر انجام تهاجم سریع به دشمن تمرکز می‌نمایند. در عالم نظری این مسئله بسیار خوب است. دیجیتالی شدن به کاربر نوعی برتری اطلاعاتی می‌دهد. درحالی‌که دشمن همچنان می‌کوشد دریابد که هرکس کجا قرار دارد، نیروی دارای سیستم دیجیتال می‌داند که هرکس کجاست و حمله کوبنده‌ای را به‌انجام می‌رساند؛ اما در عالم واقع تمامی اطلاعات نمایشگرها دقیق یا روزآمد نیستند و این مسئله منجربه حوادثی چون: به آتش بستن نیروهای خودی می‌شود. برخی میادین یا موانع جاده‌ای نیز در پایگاه‌های داده‌رسانی دیجیتال وارد نشده‌اند. این موضوع حاکی از مشکلات فناوری نوین است؛ درعین‌حال خاطرنشان می‌کند که فناوری دیجیتالی شدن با وجود سربازان آموزش‌دیده و مجرب بهترین کارکرد را دارد. اغلب سربازان امروزی با بازی‌های کامپیوتری بزرگ شده‌اند. وجه مشخص بازی‌های مزبور استفاده گسترده از اطلاعات صریح و بدون ابهام است. آنچه قرار است بدان پرداخته شود، قابل مشاهده است. در میدان جنگ مسائل این چنین روشن و واضح نیستند. درحقیقت سروکار داشتن با اطلاعات مبهم از آن دسته مهارت‌ها نیست که برای بقا در جنگ مورد نیازند؛ بنابراین نسل جدید پیش‌ازآنکه بتواند به‌طور کامل از دیجیتالی شدن در صحنه نبرد بهره گیرد، باید برخی عادات بد را ترک گوید.

هم‌اینک این مسئله در خلال اولین آزمایش‌های میدانی کامل دیجیتالی شدن درخصوص نیروهای زمینی قابل مشاهده است. در آزمایش‌های مزبور یک گردان دیجیتالی‌شده در مقابل

واحدی مجرب، اما غیردیجیتالی قرار داده شد و در نتیجه به‌صورت نوعی منحنی آموزشی نمایان گشت. فرماندهان مجبور بودند یاد بگیرند که گهگاه به اطلاعات نادرست بپردازند. سربازان نیز مجبور بودند فراگیرند که به‌سرعت به فرصت‌هایی که درک فزاینده از شبکه میدان جنگ مزبور در اختیارشان قرار می‌داد واکنش نشان دهند. پس از مقداری تمرین، فرماندهان دریافتند هنگامی‌که نادرست بودن اطلاعات شگفت‌انگیزی که بر روی صفحه مشاهده می‌کردند به اثبات رسید، چگونه به‌سرعت طرحی دیگر ارائه دهند. سربازان عادت کردند که برای حمله به دشمنان غیرقابل مشاهده (با چشم) که حسگرها و رادارها شناسایی می‌نمودند، به‌سرعت مهیا گردند. همانطورکه پیش‌بینی می‌شد، نبرد بسیار پرجنب‌وجوش‌تر، اما مؤثر بود. سربازان غیردیجیتالی وقتی آموختند که هرنوع درگیری با [illegible] می‌تواند به‌سرعت به نبردی ناامیدکننده علیه دشمنی مبدل گردد که درخصوص محل [illegible] از نیروها و کارهایی که انجام می‌دهند اطلاعات بیشتری دارد، بیشتر احتیاط کردند.

جنگ افغانستان شانس اول آزمودن دیجیتالی شدن در صحنه نبرد بود. خودروهای دارای رادار به‌صورت گسترده مورد استفاده قرار گرفتند. هواپیمای شناسایی پردیتور[1] بسیار مفید بود. هواپیمای مزبور که قادر بود دوازده ساعت یا بیشتر روی میدان نبرد پرواز کند، اطلاعات به‌دست آمده را به هواپیماهای شکاری یا نیروهای زمینی مجاور منتقل می‌نمود و دشمن در روی زمین (اگر زنده می‌ماند) متحیر می‌ماند که بلای مزبور از کجا نازل می‌گردد. هواپیمای پردیتور مسلح نیز مورد استفاده قرار گرفت که یک جفت موشک پنجاه کیلوگرمی هل فایر[2] حمل می‌کرد و می‌توانست بلافاصله بدون آنکه منتظر ظاهر شدن بمب‌افکن‌ها شود، به اهداف حمله کند. نیروهای ویژه رادیو، تجهیزات جهت‌یابی و رایانه‌های ویژه برای کنترل اوضاع جوی و نیروهای زمینی به همراه داشتند. چنانچه آنان هدف مناسبی می‌یافتند، آن هدف پیش‌ازآنکه حتی بداند شناسایی شده، مورد حمله واقع می‌شد. همچنین سیستم‌های نیروهای

1. Predator 2. Hellfire

ویژه می‌توانستند به محلی هدایت شوند که گمان می‌رفت دشمن مشغول فعالیت است. اغلب روشن نبود که اقدامات روی زمین مربوط به غیرنظامیان است یا سربازان دشمن، اما تیم‌های مزبور می‌توانستند از نزدیک نگاهی بیندازند و سپس درخواست حمله کنند. این مسئله تلفات غیرنظامی را بسیار پایین نگاه داشت؛ زیرا در گذشته هواپیماهای جنگی در منطقه جنگی همواره جانب احتیاط را رعایت می‌کردند و به هر فعالیت مشکوکی بر روی زمین (که گهگاه سربازان خودی بودند) حمله می‌کردند. این نبرد اطلاعاتی در صحنه نبرد بود که عدم توجه به آن می‌تواند ناکامی بزرگی را به‌همراه آورد.

۲. جنگ الکترونیک

کمی پس‌ازآنکه اولین پیام‌های نظامی ازطریق سیم منتقل شد، دیگر سربازان دریافتند که می‌توانند از آن به نفع خویش بهره گیرند. جنگ الکترونیک در آغاز ابتدایی بود. بریدن سیم‌های تلگراف یا استراق‌سمع مؤثر واقع می‌شد. اقدامات بعدی شامل ارسال پیام‌های ساختگی بودند. در خلال جنگ جهانی اول، رمز مورد استفاده قرار گرفت که به‌طور مداوم رمزهای مزبور کشف می‌شدند، جهت‌یاب‌های رادیویی مورد استفاده قرار می‌گرفتند و میکروفن‌هایی برای شناسایی فعالیت دشمن در میدان جنگ نصب می‌شدند. ترافیک رادیویی ساختگی نیز برای فریب تحلیل‌گران اطلاعاتی دشمن کاربرد داشت. در پایان جنگ جهانی دوم جنگ الکترونیک به عامل مهمی در طرح‌ریزی جنگی مبدل گردید. بدون طراحی نقشه فریب ارتباطی، حمله عمده‌ای طرح‌ریزی نمی‌شد. اعلام سکوت رادیویی کافی نبود و دشمن درمی‌یافت که چیزی در جریان است. بنابراین ترافیک رادیویی ساختگی به‌وجود آمد. روی رادارهای دشمن و ابزارهای جهت‌یابی پارازیت انداخته می‌شد یا آنها را فریب می‌دادند. از جنگ دوم جهانی به‌این‌سو، جنگ الکترونیک به سلاحی حساس مبدل گردیده است. آزمایش‌ها نشان داده‌اند هنگامی‌که واحدهای دشمن با پارازیت‌اندازی، جهت‌یاب‌های رادیویی کنترل‌کننده جنگ الکترونیکی و فریب الکترونیکی روبه‌رو می‌شوند، بی‌هدف و منفعل

می گردند. شگفت‌آنکه هیچ‌یک از نیروهای مسلح عمده هنوز این فرصت را نیافته‌اند که از ابزارهای جنگ الکترونیک کنونی علیه یکدیگر استفاده نمایند. سیستم‌های تحمیلی مزبور با تأثیر ویرانگر علیه کشورهای کوچک مورد استفاده قرار گرفته‌اند. هواپیماهای آمریکایی علیه ویتنام و اسرائیل در جنگ‌های خاورمیانه، الگوهای ویرانگر و مهم در این زمینه هستند. در سال ۱۹۹۱ عراقی‌ها توانستند تا حدی از تجهیزات جنگ الکترونیک خویش استفاده نمایند؛ اما این میزان برای برجای گذاردن تأثیری اساسی کفایت نکرد. استفاده از جنگ الکترونیک در زمان صلح برای آزمایش‌های میدانی اغلب تأثیر فاجعه‌باری داشته است. هنگامی‌که هر دو طرف قادر باشند در حد مطلوب از جنگ الکترونیک علیه یکدیگر استفاده نماید، انتظار می‌رود که تأثیر آن مشابه سلاح‌های هسته‌ای یا شیمیایی باشد. البته آنچنان تلفات سنگینی به‌صورت مستقیم نخواهد داشت؛ اما انتظار می‌رود سردرگمی و آشفتگی فراوانی درپی داشته باشد. با فرض وجود دلایل محکم درخصوص عدم استفاده از سلاح‌های شیمیایی یا هسته‌ای در یک جنگ قدرت عمده جنگ الکترونیک می‌تواند بیشترین اثر را در میدان جنگ در آینده بگذارد.

روسیه همواره جنگ الکترونیک را جدی می‌گرفت. به‌طور نظری، روس‌ها کمتر از نیروهای غربی به ارتباطات مستمر رادیویی وابسته بودند. دکترین نیروهای زمینی شوروی، هدایت گردان‌های رزمی خویش در جهتی معین و سپس پخش کردن آنان بود. از آنان انتظار می‌رفت تا زمانی‌که به اهداف خویش نایل نگردند، ادامه دهند یا ازمیان بروند. نیروهای شوروی بر ارتباطات غیرالکترونیکی چون: نور، پرچم و پیام‌رسان[1] تأکید زیادی می‌کردند. همچنین آنان در موقعیت‌های ایستا، از تلفن‌های محدود استفاده می‌نمودند و نیروی هوایی و ناوگان دریایی‌شان نسبت به رقبای غربی بسیار بیشتر به ارتباطات رادیویی وابسته بودند. به‌علاوه در نیروهای مسلح شوروی رسم بر این بود که بدون اخذ دستورات مفصل از فرماندهان ارشد هیچ کاری صورت نمی‌پذیرفت. واحدهای شوروی در آزمایش‌های میدانی

---

1. Messengers

بدون ارتباطات رادیویی تمرین می‌کردند؛ هرچند منتقدان نظامی آزمایش‌های میدانی مزبور را به شبیه‌سازی تشبیه می‌نمودند و معرف میدان جنگ واقعی نمی‌دانستند. در آینده بزرگ‌ترین خطر ناشی از دکترین و ماشین‌افزار جنگ الکترونیک ساخت روسیه و صادره از این کشور، استفاده کشورهای جهان سوم از آنها علیه نیروهای کشورهای غربی است. بسیاری از نیروهای مزبور طبق عادت از ارتباطات غیرالکترونیکی بیشتری استفاده می‌کنند و به اندازه ما به ابزارهای الکترونیکی وابسته نیستند. ممکن است اتحاد شوروی ازمیان رفته باشد؛ اما میراث جنگ الکترونیک آنان در آینده باقی خواهد ماند. درحالی‌که تمامی نیروهای مسلح ممکن است تصور کنند جنگ الکترونیک وابستگی آنان به تجهیزات الکترونیکی را به مخاطره می‌افکند، راه‌حل‌های الکترونیکی نیز وجود دارند. بازهم این کامپیوترها هستند که وارد عمل می‌شوند. یکی از متداول‌ترین راه‌حل‌های مسئله، استفاده از نظام فرکانس‌هایی است که توسط کامپیوتر کنترل می‌گردد که فرستنده‌ای در اختیار دارد و با استفاده از آن با سرعت بالا فرکانس‌ها را عوض می‌کند. ازآنجایی‌که پارازیت انداختن بر روی تمام فرکانس‌ها دشوار است، دستگاه تعویض فرکانس بیشتر سبب انتقال پیام می‌شود.

مشکل دفاع در مقابل جنگ الکترونیک آن است که راه‌حل‌ها تنها روی کاغذ می‌آیند و اغلب جامه عمل نمی‌پوشند. روسیه حجم زیادی از تجهیزات جنگ الکترونیک ابتدایی را ارتقا داده است؛ درحالی‌که اغلب ماشین‌افزارهای جنگ الکترونیک غربی در آزمایشگاه‌ها قرار دارند. مقدار تجهیزات جنگ الکترونیک غرب تنها در دریا و هوا زیاد است. جنگ زمینی عمده در آینده می‌تواند بسیار جالب باشد. حتی در جنگ‌های زمینی علیه ارتش‌های جهان سومی نیز چنانچه افراد از ماشین‌افزار پارازیت روسی استفاده نمایند، هراس از پیامدهای غیرقابل پیش‌بینی وجود دارد.

۲ـ۱. اجزای تشکیل‌دهنده جنگ الکترونیک

جنگ الکترونیک چندان ساده نیست و از اقدامات مجزا و متعددی تشکیل می‌گردد. هر یک از

این اقدامات به‌خودی‌خود کاملاً پیچیده است و درک این پیچیدگی، حاکی از گستردگی جنگ مذکور است.

۲ـ۱ـ۱. اقدامات نظارت الکترونیکی[1]: تنها پیگیری ابزارهای الکترونیکی دشمن به کاری عمده مبدل گردیده است؛ به‌ویژه به‌دلیل‌آنکه هیچ‌کس به‌طوردقیق نمی‌داند که تجهیزات الکترونیکی یک فرد چگونه عمل خواهد کرد، مگر آنکه طی دوره‌ای مداوم مورد استفاده قرار گیرد. چنین استفاده‌ای در زمان صلح و هنگامی‌که تجهیزات جنگ الکترونیکی به‌طور مداوم برای آموزش و آزمایش مورد بهره‌برداری قرار می‌گیرند، روی نخواهد داد. تمامی تجهیزات الکترونیکی دارای آرم الکترونیک منحصربه‌فرد هستند. حتی تجهیزاتی که پخش‌کننده نیستند نیز در مواقعی، مانند حسگرهای متعددی چون: رادار و سونار[2] عمل خواهند نمود. بنابراین یکی از کارکردهای اساسی زمان صلح تعیین این مسئله است که آرم‌های مزبور چه هستند. به‌این‌دلیل نیروی دریایی و هوایی بخش قابل ملاحظه‌ای از وقت خویش را صرف پیگیری قابلیت‌های دیگر کشورها می‌نمایند و در مقابله با اقدامات نظارت الکترونیکی هرگاه میسر گردد، تجهیزات را تغییر قیافه می‌دهند. می‌توان سیگنال‌ها را در شرایط مختلف تغییر داد. درخصوص تجهیزاتی که چون هواپیماها و کشتی‌ها می‌توان از روی شکلشان آنها را تشخیص داد، شکل و جنسشان باید به‌گونه‌ای طراحی گردد که امکان شناسایی را به حداقل برساند. این موضوع، اساس فناوری پنهان‌کاری است که ایالات متحده درخصوص تعدادی از وسایل نقلیه به‌ویژه هواپیماها اعمال می‌کند. کشتی‌ها، هواپیماها، بالگردها و خودروهای کوچک که مملو از حسگر هستند، بیشترین فعالیت جمع‌آوری اطلاعات را انجام می‌دهند. ماهواره‌هایی که در سطح پایین پرواز می‌کنند، برای دریافت سیگنال‌هایی در عمق قلمرو یک کشور مفید هستند. هواپیماهای شناسایی و نیز حسگرهای مصنوعی که روی زمین یا کف دریا کار گذاشته می‌شوند نیز مفید واقع می‌گردند.

---

1. ESM Electronic Surveillance Measures (ESM)
2. Sonar

گردآوری اطلاعات چیزی بیش از کار حسگرهاست. ابزارهای ثبت‌کننده، ترجمه‌کنندگان زبان‌های بیگانه و تجهیزات فراوری سیگنال‌ها نیز پا به عرصه وجود نهاده‌اند. رایانه‌ها به‌طور روزافزون در بررسی توده‌ای از اطلاعات موجود نقش اساسی ایفا می‌کنند. حجم گسترده داده‌ها جمع‌آوری و تحلیل می‌شوند و به مقادیر متناسبی از داده‌ها تبدیل می‌گردند تا سربازان و تسلیحات خودی بتوانند از آنها استفاده کنند. اقدامات نظارتی الکترونیکی آنچنان موفقیت‌آمیز بوده‌اند که طبقه‌ای کامل از حسگرهای فعال[1] به مخاطره افتاده‌اند. حسگرهای فعال به‌واسطه پخش سیگنال اشیا را شناسایی می‌کنند. هنگامی که سیگنال مزبور به چیزی برخورد می‌نماید، حسگر انعکاس آن را شناسایی کرده، درمی‌یابد که چیزی وجود دارد. این اساس رادار است که به انتشار امواج می‌پردازد و نیز سونار که صدا را منتشر می‌کند. به سبب پخش سیگنال، یک حسگر منفعل[2] می‌تواند آن را شناسایی کند. حسگرهای منفعل تنها گوش فرامی‌دهند. به‌دلیل‌آنکه سیگنال‌های حسگرهای فعال باید برای انعکاس برخورد با یک شیء به آن برسند، خودرویی که حسگر منفعل حمل می‌کند، خودرویی را که حامل حسگر فعال است سریع‌تر شناسایی می‌کند. این مسئله هنگامی که از شناسایی‌کننده رادار در خودروی خویش برای شناسایی رادارهای کنترل سرعت پلیس استفاده می‌کنید نیز رخ می‌دهد. معمولاً پیش‌ازآنکه رادار پلیس سرعت غیرمجاز شما را تشخیص دهد، وقت کافی برای کاهش سرعت خود را دارید. همانطورکه استفاده‌کنندگان از چنین ابزارهایی خوب می‌دانند، رقابت مستمری برای بهره‌گیری از رادارهای بهتر و اقدام علیه رادارهای شناسایی در جریان است. امروزه حسگرهای منفعل سوژه داغی را در تحقیق و توسعه تشکیل می‌دهند که دلایل آن نیز روشن است. شناسایی حسگرهای منفعل تقریباً غیرممکن است. همچنین این حسگرها قادرند طیف وسیعی از سیگنال‌ها را شناسایی کنند. حسگرهای حرارتی قادرند هرنوع حرارتی (از حرارت اندک بدن گرفته تا پوسته بسیار داغ هواپیمای جت در حال نزدیک شدن) را شناسایی نمایند. کشورها تا چه اندازه این مسئله را جدی می‌گیرند؟ چینی‌ها از

---

1. Active Sensors
2. Passive Sensor

دست هواپیمای نظارت الکترونیکی ای‌پی‌تری[1] به‌ستوه آمده‌اند؛ زیرا می‌دانستند بحث اقدامات نظارت الکترونیک در زمان صلح می‌تواند در زمان جنگ آسیب جدی به آنان وارد نماید. در اوایل جنگ سرد روس‌ها ده‌ها کشتی و هواپیمای شناسایی و نظارت الکترونیک آمریکا را سرنگون یا به آنها شلیک کردند.

عکسبرداری نیز یک حسگر منفعل مؤثر است. با استفاده از یک ابزار تلویزیونی دوربین‌مانند برای تصویربرداری و شناسایی گرما و با بهره‌گیری از مجموعه‌ای از قوای فراوری رایانه‌ای، حسگرهای مزبور قادرند در شب و میان دود و مه نیز محیط اطراف را شناسایی کنند. ماهواره‌ها و هواپیماها کاربران عمده حسگرهای تصویری مزبور را تشکیل می‌دهند. با کوچک‌تر شدن حسگرهای تصویری، در خودروهای زمینی نیز می‌توان آنها را دریافت. تانک‌های غربی مدرن از چنین ابزارهایی استفاده می‌کنند.

سونار تنها شکل حسگر صوتی نیست. درواقع اولین مورد کاربرد فناوری مزبور تخمین مسافت صوتی بود که با شمارش ثانیه‌ها میان نور آتش سلاح‌ها و شنیده شدن صدا، مسافت توپخانه‌های دور دست را تخمین می‌زد. صوت با سرعتی نسبتاً یکسان حرکت می‌کند. روش مزبور که یک قرن قدمت دارد، با فراوری سیگنال همراه شده است تا حسگرهای منفعل را برای نیروهای زمینی ایجاد نماید. در شرایط و قالب واحدی یکسان، حسگرهای لرزه‌نگار نیز مورد استفاده قرار می‌گیرند که به صدای انتقال‌یافته ازطریق زمین توسط خودروهایی که نزدیک می‌شوند گوش فرامی‌دهند. حسگرهای صوتی و لرزه‌نگار را که اغلب به همراه یک پخش‌کننده رادیویی بسته‌بندی می‌شوند، با هواپیما، توپخانه، گلوله توپ یا حتی دست به پشت خطوط دشمن پرتاب می‌کنند. حسگرهای مزبور برای انجام فعالیت در آنجا می‌مانند. وقتی چیزی شناسایی می‌شود، مجموعه داده‌های کوتاه با تراکم بالا به‌سرعت ازطریق امواج رادیویی بازتاب می‌گردد. این روش انتقال به‌منظور اجتناب از شناسایی حسگر توسط دشمن مورد استفاده قرار می‌گیرد. حسگرهای مزبور گهگاه برای جمع‌آوری

---

1. EP-3

طلاعات پوشش گیاهی طراحی می‌شوند و یافتن آنها ساده‌تر است. در طی جنگ ویتنام، شکل بتدایی حسگر مزبور مورد استفاده قرار می‌گرفت.

طی ده سال اخیر، حسگرهای مزبور بیشتر با انواع تسلیحات ترکیب شده‌اند. مین‌های دریایی بیش از پنجاه سال است که از روش‌های گفته‌شده استفاده می‌کنند. هم‌اینک ابزارهای الکترونیکی بسیار کوچک سبب گردیده‌اند که مین‌های زمینی خود دارای حسگر شوند. خودروها به‌ویژه خودروهای سنگینی چون تانک سروصدای زیادی ایجاد می‌کنند. برخی مین‌ها ـ که به‌تازگی تولید شده‌اند ـ می‌توانند تشخیص دهند که چه زمان یک تانک از روی آنها رد می‌شود تا چاشنی کوچکی که پوشش نازک کف خودرو زرهی را سوراخ می‌کند، آتش نمایند. دیگر سیستم‌ها، پرتابه‌ای موتورمانند شلیک می‌کنند که به‌نوبه‌خود خودروی زره‌پوش را شناسایی و پرتابه‌ای را به پوشش زرهی نازک سقف خودرو شلیک می‌نماید. درحالی‌که پیش‌ازاین به چندین تن مین برای نابود کردن یک تانک احتیاج بود، هم‌اینک تنها چندصد کیلوگرم مورد نیاز است. این مسئله کارایی را بیست برابر کرده است. گرچه مین‌های جدید ده برابر گران‌تر هستند، وزن عاملی حیاتی در میدان جنگ است؛ زیرا نمی‌توان حجم زیادی از مهمات را به صحنه جنگ برد.

حسگرهای منفعل درحال مبدل شدن به نوع غالب هستند. برد آنها نسبت به حسگرهای فعال محدود است؛ اما توانایی پنهان ساختن خود از دشمن برتری ارزشمندشان محسوب می‌شود. پروژه‌های حسگر در غرب در زمینه برتری فناوری عرصه الکترونیک و رایانه سرمایه‌گذاری بسیاری می‌نمایند تا حسگرهای منفعل برد بیشتری بیابند. به‌علاوه تسلیحات کنترل‌شده توسط رایانه قادرند با برنامه‌ریزی مجدد دستورات و فرامین به‌سرعت تغییر نمایند. تغییرات در عرصه نبردهای کنونی و آینده حتی سریع‌تر نیز می‌شود.

۲ـ۱ـ۲. اقدامات متقابل الکترونیکی[1]: تسلیحات الکترونیک، ابزارهای دفاعی الکترونیک را به‌همراه آوردند. طیف گسترده روش‌های مزبور ابزارهای الکترونیک را فریب داده یا در آنها

---

1. ECM Electronic Counter Measures

ایجاد اختلال می‌کنند. ایجاد پارازیت یکی از انواع آشکارتر اقدامات متقابل الکترونیکی است که شامل پخش سیگنال بلند روی همان فرکانسی است که دشمن برای انجام ارتباطات مورد استفاده قرار می‌دهد.

پارازیت‌اندازی پیچیده‌تر سبب می‌گردد که تجهیزات دشمن خراب به‌نظر برسد یا داده‌های غلط نشان بدهد. پارازیت‌اندازی مجازی با ابری از نوارهای فلزی ایجاد و سبب می‌گردد رادار فکر کند که ابر حاصله، هدف است. شعله‌ها همین کار را درخصوص حسگرهای (حرارتی) گرمایاب انجام می‌دهند. مولدهای سروصدای الکترونیکی نیز موشک‌های دارای حسگرهای منفعل را که برای هدف‌گیری حسگرهای فعال مهیا گردیده‌اند منحرف می‌سازند.

۲ـ۱ـ۳. ضد اقدامات متقابل الکترونیکی[1]: موارد مزبور روش‌های متفاوت برای مقابله با اقدامات متقابل الکترونیکی هستند. یکی از روش‌های ساده آن گرداندن فرستنده و ایجاد اختلال در پارازیت‌اندازی دشمن است. نوع عملی‌تر آن، فرستنده فورانی است: پیام در فوران مختصر، اما قدرتمند انرژی فشرده و فرستاده می‌شود. فرکانس خودکار به راه‌حلی استاندارد با فناوری بالا برای پارازیت‌اندازی مبدل گردیده است. دو فرستنده با رایانه درونی یکسان درحین انتقال و دریافت فرکانس‌ها به‌سرعت آنها را تغییر می‌دهند. همچنین از نرم‌افزار رایانه می‌توان برای بازسازی تمامی قسمت‌های پیامی که روی آن پارازیت افتاده است استفاده نمود. برای پارازیت انداختن بر یک نظام فرکانس باید روی تعداد زیادی از فرکانس‌ها پارازیت انداخت که مستلزم تجهیزات فراوان و نیروی بسیار است؛ در عرصه نبرد این دو مقوله بسیار اندکند.

دیگر شکل مستقیم ضد اقدامات متقابل الکترونیکی، مجهز نمودن مرشک‌ها به بیش از یک نوع سیستم هدف‌یاب است. گرچه گران تمام می‌شود، برخی موشک‌ها دارای رادار، هدف‌یاب رادار و ابزارهای حرارت‌یاب هستند که البته روی هر سه مورد می‌توان پارازیت انداخت.

---

1. Electronic Counter-Countermeasures (ECCM)

۲ـ۱ـ۴. *فراوری سیگنال*[1]: این مورد به مؤلفه‌ای عمده و حیاتی در جنگ الکترونیکی مبدل گردیده است. فراوری سیگنال که نیروی انسانی برای انجام آن به سال‌ها وقت نیاز دارد توسط رایانه به سادگی انجام می‌گیرد؛ برای مثال، عکس‌خوان رایانه‌ای، الگوهایی را که معرف انواع خاص استحکامات و ادوات دشمن هستند شناسایی می‌کند. هزاران سال قبل، گروه‌های شناسایی فراگرفتند که با شکل رد پاهایی که اسب‌ها برجای می‌نهادند، تشخیص دهند که به کدام سپاه تعلق دارند. هنوز با بررسی رد پایی که تانک‌ها بر زمین برجای می‌گذارند، می‌توان چنین کرد. وقتی رایانه‌ها پا به عرصه نهادند، امکان دنبال نمودن الگوها میسر گردید. به‌علاوه می‌شد الگوهای پیچیده‌تر را شناسایی نمود و به خاطر سپرد. صداهای حاصله توسط کشتی‌ها یا سیگنال‌های منتشره توسط رادارها نیز چون اثر انگشت منحصربه‌فرد هستند و هم‌اینک رایانه‌ها تشخیص آثار انگشت، شست و کف دست و حتی الگوهای چشمی برای سیستم‌های امنیتی را برعهده دارند. با کوچک‌تر شدن رایانه‌ها، فراوری سیگنال‌ها در جاهایی‌که پیش‌ازآن جای کافی وجود نداشت، مانند سیستم‌های هدایت موشک‌ها یا سازوکار کنترل آتش تانک‌ها و کشتی‌ها میسر گردید. اولین مورد استفاده چشمگیر از فراوری سیگنال رایانه‌ای در سونارهای منفعل بود. اقیانوس محل پر سروصدایی است و لایه‌های متعدد آب با دماهای متفاوت دارد که سبب می‌گردد صدا پخش شده، حتی منحرف گردد. تشخیص صدای زیردریایی توسط کشتی‌های بازرگانی ابتدا با فراوری سیگنال میسر شد. حجم وسیعی از صداها در حافظه رایانه‌ها نگهداری می‌شود و در مقاطع زمانی مختلف روزآمد می‌گردد. بنابراین هر کشتی را با مسیر حرکت و سرعتش می‌توان شناسایی نمود. همین مسئله درخصوص تشخیص سریع و دقیق سیگنال‌ها در هوا و زمین صادق است. نیروی هوایی از فراوری سیگنال برای تشخیص سیگنال‌های رادیویی و رادار بهره می‌گیرد و هواپیما را قادر می‌سازد تا از سلاح‌های ضدهوایی و هواپیماهای رهگیر دوری

1. Signal Processing

نماید. اهداف و مناطقی که با رادارهای خودی پوشش داده می‌شوند نیز راحت‌تر قابل شناسایی هستند. واحدهای زمینی از فراوری سیگنال برای دفاع هوایی و جمع‌آوری اطلاعات استفاده می‌کنند. انواع دیگر فراوری سیگنال، تحلیل ترافیک رادیویی، مطالعه و بررسی الگوهای سابق پیام‌های دشمن و استفاده از حسگر هستند. برای عملیات‌های مختلف مانند: آمادگی حمله یا دفاع، الگوهای متفاوتی نیز مورد بررسی قرار می‌گیرند. آخرین جنبه فراوری سیگنال آن است که برتری قابل ملاحظه کشورهای غربی بر دیگر ملل در فناوری رایانه‌ای سبب می‌گردد تسلیحات مزبور، به‌طورعمده غربی به‌شمار آیند.

۲ـ۱ـ۵. *اقدامات فریب الکترونیکی*[1]: موارد مزبور مجموعه‌ای از روش‌ها برای فریب دشمن هستند. می‌توان فرستنده‌ها را تنها برای منحرف نمودن دشمن یا شبیه‌سازی وجود یکی از واحدهای خودی ـ که وجود ندارد ـ مورد استفاده قرار داد. ترافیک پیام‌های رادیویی شبیه‌سازی شده می‌تواند نشانگر آن باشد که واحدی در تدارک حمله است؛ درحالی‌که درواقع درحال نقل مکان به جای دیگر است. کهن‌ترین روش فریب ارسال پیام‌ها به‌صورت رمز است. رمزنگاری تقریباً به‌طورکلی به ابزارهای الکترونیک وابسته است. رایانه‌ها رموز را تشخیص می‌دهند و می‌کوشند آنها را بشکنند؛ بدین‌منظور حسگرها به‌طور مداوم رمزهای دشمن را بررسی می‌کنند و به‌دنبال انواع جدیدی می‌گردند. روش‌های ساده‌تر، ارزان‌تر و اغلب مؤثرتری وجود دارند و بر این پایه استوارند که چه مدت زمانی پخش پیام‌ها به‌طول می‌انجامند. رادارهای جدیدتر آنقدر دقیق هستند که برای چند ثانیه روشن می‌شوند و سپس تا یک دقیقه یا بیشتر پیش‌ازآنکه دوباره روشن شوند، اطلاعات را ردوبدل می‌نمایند. فوران‌های کوتاه رادارهای مزبور می‌تواند برای غلبه بر اغلب پارازیت‌ها به اندازه کافی قدرتمند باشد و این مسئله نشان می‌دهد که سادگی اغلب مؤثرترین راه‌حل است.

1. Electronic Deception Measures (EDM)

۲ـ۲. رویکردها در جنگ الکترونیک

۲ـ۲ـ۱. جنگ الکترونیک تهاجمی

وقتی نیرویی حمله می‌کند، جنگ الکترونیک چند کارکرد اساسی را فراهم می‌آورد:

• **یافتن هدف:** حسگرها، نظارت الکترونیک و فراوری سیگنال به تلاش برای تشخیص فعالیت، قدرت و موقعیت واحدهای دشمن کمک می‌کنند و از فهرست مزبور اهداف حیاتی برای حمله انتخاب می‌شوند.

• **ایجاد اختلال در فرماندهی، کنترل و ارتباطات:** پارازیت انداختن بر روی ارتباطات دشمن، ارسال پیام‌های نادرست و تخریب تجهیزات ارتباطی دشمن مانع از آن می‌گردد که وی به‌طور مؤثر با حمله مقابله نماید.

• **فریب:** فریب الکترونیک پیش از حمله، دشمن را درخصوص نیات واقعی گمراه می‌نماید.

۲ـ۲ـ۲. جنگ الکترونیک دفاعی

در جنگ الکترونیک، دفاع بسیار مهم‌تر از تهاجم است. به‌دلیل‌آنکه همگان به فرستنده‌ها و حسگرها بسیار وابسته هستند، تخریب ابزارهای مزبور می‌تواند بسیار جبران‌ناپذیر باشد. خوشبختانه جنگ الکترونیک به‌طور مداوم در فرستنده‌ها و حسگرها ایجاد اختلال نمی‌کند. تجهیزات پازایت‌اندازی گران هستند و هنگام استفاده ناخواسته توجه فراوانی را جلب می‌نمایند. موشک‌های ضدحرارتی به‌راحتی می‌توانند پارازیت‌اندازانی را که به‌صورت مستمر پارازیت می‌اندازند، رهگیری کنند. دستگاه‌های پارازیت بیشتر هنگامی مورد استفاده قرار می‌گیرند که عملیات مهمی (اغلب عملیات تهاجمی) درحال انجام باشد.

• **ارتباطات جایگزینی:** فرستنده‌های رادیویی جایگزین‌هایی چون: پیام‌رسان‌ها، تلفن‌های ثابت و سیار و منورها دارند. تمامی این موارد به‌اندازه فرستنده سریع و انعطاف‌پذیر هستند. جهت استفاده از آنها باید مهیا شد که عملیات‌ها را نیز طبق آنان تنظیم نمود. حسگرهای

جایگزین با قدرت کمتر نیز موجودند که شامل: پست‌های دیده‌بانی، منورهای تله‌ای و میادین مین هستند. مسئله مهم آمادگی برای ازدست دادن قابلیت طبیعی فرستنده و حسگر است؛ زیرا بدترین وضعیت ممکن برای مدافع غافلگیر شدن است.

• **نظم ارتباطات:** به‌دلیل‌آنکه نظارت الکترونیک یکی از اقدامات جنگ الکترونیک است که به‌طور مستمر صورت‌می‌پذیرد، باید بیش از همه از آن واهمه داشت. چنانچه سربازان عادت کنند به شیوه‌ای قابل پیش‌بینی و یکسان از فرستنده‌ها و حسگرها استفاده کنند، دشمن به‌زودی به آن پی برده، قادر خواهد بود که واحدها و تأسیسات حساس و کلیدی را شناسایی کند و در مراحل اولیه حمله به آنها یورش برد یا پارازیت بیندازد.

• **نظارت الکترونیک:** نظارت الکترونیک بسیار اساسی و حساس است؛ زیرا اگر آن را درست به انجام برسانید، خواهید دانست که دشمن درصدد انجام چه کاری است. عدم غافلگیری بیش از نیمی از دفاع الکترونیک مؤثر را تشکیل می‌دهد.

• **تقویت تجهیزات:** انفجارات هسته‌ای حجمی از انرژی الکترومغناطیسی ایجاد می‌کند که تجهیزات الکترونیک را از کار انداخته، یا نابود می‌کند. انفجار هسته‌ای یک مگاتنی در جو زمین تجهیزات الکترونیکی را هزاران کیلومتر آن طرف‌تر از کار خواهد انداخت. هم‌اینک تجهیزات انفجاری غیرهسته‌ای وجود دارند که چنین کاری را در مسافت کوتاه‌تر (چندین کیلومتر) انجام می‌دهند؛ اما تأثیرات مهلک آن بر تجهیزات الکترونیک به همان اندازه است. از برخی تجهیزات مزبور می‌توان طی چند دقیقه یا چند ساعت به‌طور مجدد استفاده نمود؛ ولی بقیه برای همیشه از کار می‌افتند. انفجارات نزدیک‌تر تجهیزات بیشتری را از میان می‌برند. با پوشاندن تجهیزات و سخت‌تر کردن پوسته آنها برای مقاومت در مقابل حجم انرژی مزبور می‌توان از اغلب موارد مذکور جلوگیری کرد. چنین اقداماتی قیمت تجهیزات را حدود پنج درصد افزایش می‌دهد. تقویت تجهیزات به امری متداول تبدیل شده است. تنها کشورهای اندکی به تمامی ابزارهای فوق دسترسی دارند. کشورهایی که از لحاظ فنی عقب‌مانده‌تر هستند با راهبردهای هوشمندانه متعددی سعی در جبران این نقیصه دارند.

۲ـ۲ـ۳. پارازیت‌اندازی سدکننده[1]

بسیاری از کشورها که فاقد ابزارهای پارازیت‌اندازی پیچیده‌ای هستند که توسط کشورهای غربی تولید می‌شوند، از پارازیت‌اندازی سدکننده برای بسیاری از فرکانس‌ها استفاده می‌کنند. آنها قادرند مولدها و دستگاه‌های پارازیت ساده بسیاری تولید کنند تا این کار را به انجام رسانند. همچنین تجهیزات جهت‌یاب بیشتری را به میدان نبرد می‌آورند.

• **تجهیزات پنهان:** بسیاری از دشمنان بالقوه، جوامع بسته با جنون فریب و پنهانکاری هستند. کشورهایی ازاین‌دست برخی تجهیزات را از سربازان خود نیز پنهان می‌دارند؛ از بیم آنکه سربازانشان به سرعت قادرند طرز استفاده از آنها را فراگیرند و دشمن نیز کمی دیرتر قادر به انجام این کار خواهد بود. رویکرد مزبور در قرن پیش به‌طور موفقیت‌آمیزی مورد استفاده قرار گرفته است. می‌توان مطمئن بود که تمامی تجهیزات جنگ الکترونیک بسیاری از کشورها برای دشمنان احتمالی آنان شناخته شده نیست.

۲ـ۲ـ۴. سیستم‌های اضافی

به‌نظر می‌رسد که کشتی‌ها، هواپیماها و واحدهای زمینی بسیاری از کشورها تجهیزات بیشتری نسبت به رقبای غربی خویش دارند. این مسئله تا حدی به این دلیل است که نمی‌توانند تجهیزات خویش را به خوبی سربازان غربی نگهداری کنند و نیز این امر به آنها در عرصه نبرد گزینه‌های بیشتری می‌دهد. چنانچه سیستمی با اقدامات متقابل غربی‌ها از کار افتد، شاید سیستم متفاوت بتواند کاری از پیش ببرد. این ایده هرچند ابتدایی، اما مؤثر است.

• **جاسوسان:** بسیاری از کشورها که به‌طور سنتی نسبت به ایالات متحده تمایل بیشتری برای استفاده از جاسوسان دارند، دریافته‌اند که می‌توان وجود نقص در بخش جاسوسی الکترونیک را با جاسوسان انسانی بیشتر جبران نمود.

برای مقابله با بسیاری از اقدامات مزبور کشورهایی که مجهزتر هستند، همچنان تجهیزات

---

1. Barrage Jamming

انعطاف‌پذیرتری دارند. ماشین‌افزار جنگ الکترونیک را که توسط رایانه کنترل می‌گردد، می‌توان به‌سرعت دوباره طراحی نمود. نیروهای غربی به‌طور روزافزون بر روی این مسئله سرمایه‌گذاری می‌کنند.

۲ـ۲ـ۵. نظریه و عمل

به یاد داشته باشید که عملکرد تجهیزات الکترونیک به‌رغم کارایی ظاهریش چیزی نسبی است. هرکس که گهگاه عملکرد نادرست رادیو، رایانه و تلویزیون را تجربه کرده باشد، شاهد این مسئله نیز بوده است. هر دستگاه الکترونیکی که ازطریق هوا به ارسال سیگنال می‌پردازد، باید با مداخلات طبیعی دست‌وپنجه نرم کند. در نتیجه مشخصات تجهیزات بسیار گمراه‌کننده و فریب‌دهنده هستند. راداری که گفته می‌شود صد کیلومتر برد دارد، هرگونه هدفی در آن برد را شناسایی نخواهد کرد. مشخصات مفصل‌تر دستگاه نشان خواهند داد که به‌ازای صد کیلومتر، اهدافی با اندازه معین (معمولاً بزرگ) در نود درصد موارد شناسایی می‌شوند و در پنجاه کیلومتر تا ۹۹ درصد آنها مورد شناسایی قرار می‌گیرند. در عمل، احتمال تشخیص در صد کیلومتر ممکن است زیر ده درصد و در پنجاه کیلومتر تنها پنجاه درصد باشد؛ این ایده اصلی فناوری پنهانکاری را تشکیل می‌دهد: چیزی را برای رادار نامرئی نکنید و تنها تشخیص آن را دشوارتر نمایید. ازآنجاکه تشخیص برای آنکه مفید واقع شود، باید استمرار داشته باشد، هدفی که روی صفحه رادار چشمک می‌زند احتمال کمتری دارد که توسط یک موشک رهگیری شده و مورد اصابت قرار گیرد. صحنه نبرد الکترونیک دنیای احتمالات است و نه قطعیات، و پیروزی نصیب طرفی خواهد شد که هنگامی‌که ماشین‌ها طبق مشخصات نوشته شده خویش عمل نمی‌کنند، به بهترین وجه با مشکل کنار آید. اما با ارزان‌تر شدن تجهیزات الکترونیک، مجهز نمودن وسائلی چون: بمب‌ها با سیستم‌های پشتیبانی میسر گردیده است. بمب‌های هوشمند که از سیگنال‌های ماهواره‌ای جی‌پی‌اس[1] بهره می‌گیرند، اغلب دارای سیستم پشتیبانی

---

1. GPS

هستند که به‌واسطه میکروالکترونیک ارزان‌تر، استفاده از فناوری قدیمی‌تر برایشان میسر شده است. حتی بمب‌ها و موشک‌ها خود دارای رایانه‌های جهت‌یابی هستند که به‌طور مستمر سیستم را برای یافتن نقص‌ها آزمایش می‌کنند و درصورت بروز نقص آن را به تکنسین‌ها یا کاربران گزارش می‌دهند. بنابراین تجهیزات الکترونیکی قوی‌تر قابل اعتمادتر هستند.

اما مشکلات جنگ الکترونیک تا حد زیادی با وحشت‌های ناشناخته نبرد اطلاعات جایگزین گردیده است. جنگ الکترونیک حدود یک قرن جریان داشته است و مردم به آن عادت کرده‌اند. آنچه نبرد اطلاعات می‌خوانیم به‌جز یک عامل آن، یعنی اینترنت بیش از این مقدار جریان داشته است. اینترنت پدیده‌ای نوین است (حداقل به‌عنوان یک شبکه غول‌پیکر جهانی) و بسیار بیش از تلفن کاربرد دارد. در واقع مردم از افراد دردسرآفرینی که نه‌تنها با اینترنت، بلکه با شبکه‌های متعدد دیگر اقدامات رذیلانه انجام می‌دهند، هراس دارند. یکی از شبکه‌های مزبور، یعنی شبکه بین‌المللی تلفن به‌واقع بزرگ‌تر و گسترده‌تر از اینترنت است. درحالی‌که اینترنت ازطریق خطوط تلفن به خانه‌ها و ادارات راه می‌یابد، اغلب روی شبکه‌های الکترونیکی جداگانه جریان دارد. همچنین بسیاری از شبکه‌های جداگانه و حیاتی دیگر که اغلب آنها در نوع خود بی‌نظیر هستند نیز وجود دارند. سازمان سیا، اینترنت خصوصی متعلق به خویش را در اختیار دارد (مانند اینترنت است و مثل آن کار می‌کند؛ اما به هیچ‌وجه به اینترنت مرتبط نیست) و دیگر دولت‌ها و سازمان‌های تجاری نیز به‌نظر قصد انجام کاری مشابه دارند. مشکل اینجاست که به‌هرروی افراد بدخواه درصدد نفوذ هستند. کل نکته فناوری اینترنت وجود استاندارد و معیاری برای انتقال اطلاعات است؛ اما شبکه‌های مستقل حجم زیادی از مشکلاتی که کاربران بدخواه ایجاد می‌کنند از میان می‌برند. کاهش مشکل برای ارتش میسر اما حذف آن غیرممکن است (یا ارزش آن را ندارد). مشکل عمده نبرد اطلاعات این است که تاکنون هیچ جنگ نظامی عمده‌ای که تمامی ابعاد استفاده از تسلیحات نبرد اطلاعات را دربرداشته باشد به‌وقوع نپیوسته است. گهگاه درگیری‌هایی وجود داشته است؛ در آوریل ۲۰۰۱ نفوذگران چینی جنبشی معروف را آغاز کردند تا در اعتراض به برخورد هواپیمای

سوخت‌رسان آمریکایی با جنگنده چینی، پایگاه‌های اینترنتی ایالات متحده را تخریب کنند. چینی‌ها دراین‌خصوص خوب عمل نکردند و تنها سیصد پایگاه را مورد هجوم قرار دادند؛ درحالی‌که نفوذگران آمریکایی برای تلافی بیش از نهصد پایگاه اینترنتی چین را ازکار انداختند. به‌ظاهر نفوذگران چینی که تسلیم نشده بودند، مسئول انتشار کرم اینترنتی رمز قرمز[1] بودند که بیش از سیصد هزار پایگاه اینترنتی (بیشتر آمریکایی) را ازکار انداخت. دانشگاهی در چین منشأ رمز قرمز بود. چین آشکارا اعلام نمود که جنگ مجازی یکی از حوزه‌هایی است که این کشور قادر است در آن به قابلیت جهانی برسد و با آمریکا برابری نماید. بسیاری از حملات شبکه به اهداف ایالات متحده منشأ چینی داشت که اغلب سرورهای دولتی چین بودند. نمونه دیگر جنگ مجازی این کشور در نبردهای اینترنتی میان نفوذگران چینی و تایوانی طی سالیان اخیر مشاهده می‌شود. مناقشه میان چین و تایوان بر سر استقلال تایوان بیش از همه روی شبکه اینترنت مشهود بوده است.

اقدامات مزبور اغلب توسط افراد رده پایین انجام می‌گرفت که پایگاه‌های اینترنتی یکدیگر را تخریب می‌کردند؛ اما نشانه‌هایی از اقدامات جدی‌تر نیز وجود داشته است. حملات اینترنتی بسیار تخریب‌کننده نیازمند تمهیدات زیاد و اغلب مشتمل بر نفوذ کاملاً آرام به رایانه‌های قربانیان برای شناسایی ابزارهای تدافعی و گهگاه پیاده نمودن برنامه‌هایی برای استفاده بعدی هستند. امروزه جنگجویان مجازی چینی بسیاری وجود دارند که در اینترنت به این‌سو و آن‌سو می‌روند.

به جز ناشناخته‌های نبرد اطلاعات، این مشکل نیز وجود داشته که اغلب تسلیحات مجازی دوره عمر کوتاهی دارند. تسلیحات نبرد اطلاعات به نقص‌های نرم‌افزاری وابسته هستند که به‌طور مستمر شناسایی و ترمیم می‌شوند؛ اما این چیزی است که چین در آن تبحر دارد و با افزایش تعداد مهندسان و نفوذگران نرم‌افزار ماهر، قابلیت این کشور برای شناسایی و سوءاستفاده از نقص‌های اینترنت بیش از دیگر کشورها افزایش می‌یابد.

---

1. Cod Red Worm

بدترازهمه اینکه چین در پشتیبانی از این نوع نگرش کم‌هزینه نبرد اطلاعات پرده‌پوشی نکرده است. درحالی‌که باید به برخی جنگجویان مجازی این کشور که در ستادهای جنگ مجازی مستقرند، حقوق پرداخت گردد، قسمت اعظم کار توسط داوطلبان میهن‌پرستی انجام می‌گیرد که از میان تعداد روزافزون مهندسان و برنامه‌نویسان نرم‌افزار کشور برخاسته‌اند. شوق جنگجویان مجازی مذکور در برخورد با تایوانی‌ها مشاهده می‌شود که داوطلبانه برای دفاع از سرزمین اصلی وارد کارزار شده‌اند. تنها نکته روشن در این مسئله تایوانی‌ها هستند که به خوبی از موضع خویش در خطوط مقدم جنگ مجازی پیش رو آگاهند. بنابراین قسمت اعظم اقدامات در حوزه نبرد اطلاعات در سایه انجام می‌گیرد. هرکس باید تسلیحات جدید و ابزارهای تدافعی جدیدی به‌وجود آورد؛ زیرا نرم‌افزاری که اینترنت را به پیش می‌راند یا تجهیزات جنگ الکترونیک، به‌طور مستمر درحال تغییرند. هنگامی‌که مطمئن نیستید دشمن چه تسلیحاتی در اختیار دارد، اقدام به نبرد اطلاعات دشوار است. مراحل آغازین نبرد اطلاعات در آینده مملو از شگفتی خواهد بود؛ چنانچه واقعاً آماده باشید اغلب شگفتی‌ها برایتان خوشایند است.

۲ـ۲ـ۶. آینده

با ارزان‌تر شدن ابزارهای الکترونیکی، تسلیحات نیز ارزان و ارزان‌تر می‌شوند. یک نمونه بمب هدایت‌شونده جی‌دام[1] است که اولین‌بار در جنگ افغانستان مورد استفاده قرار گرفت. کیت بمب مزبور ـ که با سیگنال‌های ماهواره جی‌پی‌اس هدایت می‌شود ـ تنها هجده هزار دلار قیمت دارد و قسمت اعظم آن مربوط به عامل مکانیکی است که باله‌هایی که بمب مزبور را هدایت می‌کنند، کنترل و تغذیه می‌کند. تجهیزات الکترونیک جی‌پی‌اس کمتر از یکصد دلار قیمت دارند. این یکی از فرصت‌هایی است که تحول روبه‌رشد رایانه‌های کوچک در عرصه طراحی و ساخت تسلیحات فراهم آورده است. برای آنکه قدر گسترده تحولات مزبور را بدانیم، باید هزینه‌های قدرت محاسبه در طی چند دهه گذشته را مدنظر قرار دهیم.

---
1. JDAM

ام‌آی‌پی‌اس[1] (تعداد میلیون دستورات و فرامینی که یک رایانه در هر ثانیه قادر به انجامشان است) یکی از معیارهای اندازه‌گیری قدرت محاسبه به شمار می‌رود. در اواسط دهه هفتاد، قدرتمندترین رایانه‌های موجود می‌توانستند یک ام‌آی‌پی‌اس ـ که پنجاه‌هزار دلار قیمت داشت ـ در اختیار داشته باشند. کامپیوترهای کوچک و ایستگاه‌های کاری رایانه‌ای با زیر صد ام‌آی‌پی‌اس با قیمت هزار دلار برای هریک کار می‌کردند و رایانه‌ای کوچک‌تر با بیش از بیست ام‌آی‌پی‌اس با قیمت زیر پانصد دلار کار می‌کردند. در سال ۲۰۰۱ قیمت هر ام‌آی‌پی‌اس به زیر ده دلار رسید و همچنان درحال پایین آمدن بود. با پایین آمدن هزینه محاسبه، ریزپردازنده‌ها در تجهیزات و تسلیحات بیشتری نمایان می‌گردند. رادیوها، بمب‌ها، خودروها، دوربین‌های دوچشمی و حتی اجاق گازهای خانگی دارای رایانه شده‌اند. ارتش آمریکا به تحقیقات دراین‌خصوص یارانه داده است تا برای استفاده سریع در حسگرها و تسلیحات موجود و نوین، رایانه‌های کوچک سریع‌تری تولید شوند. هم‌اینک میزان بسیار زیاد محاسبات را می‌توان سریع و ارزان به انجام رسانید که این یک قابلیت مهم تلقی می‌گردد. با ایجاد قابلیت برای تولید نرم‌افزارهای جدید برای استفاده سریع و آسان در ماشین‌های دارای رایانه‌های کوچک این مسئله روند بسیار سریع‌تری یافته است. ارتش آمریکا با خرید صدها هزار دستگاه از جدیدترین رایانه‌های کوچک غیرنظامی و توزیع آزادانه آنها در این زمینه پیشگام بوده است. همانطورکه بسیاری از سربازان آمریکایی و کانادایی در جنگ جهانی دوم به‌دلیل قابلیت راندن خودرو بر دیگران برتری داشتند، هم‌اینک نیز به‌دلیل قابلیت استفاده بسیاری از سربازان ایالات متحده از کامپیوترهای کوچک و برنامه‌نویسی، چنین مسئله‌ای درحال رخ دادن است. روند مزبور از اواخر دهه هفتاد به‌این‌سو، هنگامی‌که سربازان با پول خود اولین رایانه‌های کوچک را خریداری کردند و وظایف نظامی خود را ماشینی نمودند، ادامه داشته است. ارتش‌های غربی با گردش کوتاه سیستم تدارکات خویش از وضعیت مزبور بهره گرفته و غیرنظامیان با افزودن

---

1. MIPS

سپر محافظ و ضدضربه کردن رایانه‌های کوچک، رایانه‌هایی تولید کرده‌اند که پنج سال زودتر از آنکه تجهیزات مزبور در اختیار ارتش قرار گیرد پدیدار شدند و یک‌چهارم آن قیمت داشتند. در برخی موارد، آنان قادر بودند تجهیزات نظامی را که از تجهیزات غیرنظامی ضعیف‌تر بوده و ده برابر آنها قیمت داشتند تعویض نمایند.

چنانچه از وجود این حقیقت که رایانه‌ها قابل برنامه‌ریزی مجدد هستند بهره‌برداری گردد، کل قدرت رایانه‌ای اضافی مزبور با تأثیر بیشتری عمل می‌کند. برنامه‌های رایانه‌ای به‌سادگی تهیه نمی‌شوند؛ اما قابلیت آن را دارند که به‌سرعت با هم ادغام و روزآمد شوند. رایانه‌ها و برنامه‌هایشان دیگر تجهیزات الکترونیکی را به‌طور روزافزون کنترل می‌نمایند. برتری غرب در فناوری رایانه‌ای به‌نظر برتری حیاتی در طیف کلی تجهیزات الکترونیک به‌شمار می‌رود. نمونه اخیر، سیستم‌های اقدامات متقابل الکترونیکی هستند که ویژگی‌های رادارهای دشمن را ذخیره می‌کنند و سپس به‌سرعت آنها را شناسایی کرده، رویشان پارازیت می‌اندازند. نیازی به برنامه‌ریزی مجدد ابزارهای مذکور نیست و تنها باید فایل داده‌هایی که تجهیزات الکترونیکی دشمن را شناسایی می‌کنند به‌روز نمود. رادارها و سونارها بیشترین نفع را از رایانه‌های قدرتمندتر و ارزان‌تر می‌برند. این بدان سبب است که مشکل اصلی رادارها پخش سیگنال نبوده، بلکه تفسیر درست سیگنال‌های ضعیف‌تری است که از هدف بازمی‌گردند. قسمت اعظم فناوری پنهانکاری غرب همچنان بر پایه ضعف فناوری رادار (اغلب روسی) قرار دارد. ساخت رادارهایی که قادرند هواپیماهای پنهان را شناسایی کنند امکان‌پذیر است؛ اما باید رایانه‌هایی در اختیار داشت که برای تفسیر درست سیگنال‌ها و فرستادن سیگنال‌های صحیح در وهله اول به اندازه کافی قدرتمند باشند. همچنین قدرت رایانه‌ای مزبور سبب می‌گردد رادارهایی با برد بسیار برای کشتی‌ها و واحدهای ضدهوایی، قابل استفاده شوند. ایالات متحده بسیاری از تجهیزات الکترونیکی نوین را برای سربازان فراهم می‌نماید. درحالی‌که بسیاری از آنها مضحک به‌نظر می‌رسند، درطی چند دهه پیش نشانه‌های خوبی از موفقیت دیده شده است. درواقع بحث به جایی رسیده است که دغدغه اصلی افسران تدارکات، تأمین باتری مورد نیاز سربازان است.

فصل هفتم

فناوری‌های زیست‌سنجی

- درآمد
- کارایی و کارآمدی سیستم‌های زیست‌سنجی
- نتایج قانونی و و سیاسی

۱. درآمد[1]

از ۱۱ سپتامبر ۲۰۰۱ علاقه بسیار زیادی در استفاده از سیستم‌های زیست‌سنجی[2] برای احراز هویت به‌وجود آمده[3] و به‌خصوص در حوزه‌های اسناد ویزا و مهاجرت و برنامه‌های دولتی کارت شناسایی شدیدتر است.[4] برخلاف روش‌های معمولی تعیین هویت که مستلزم آن است که هر فرد ابزار شناسایی (کارت شناسایی، شماره شناسایی شخصی یا پاسپورت) به‌همراه داشته باشد، اطلاعات زیست‌سنجی جزئی از خود افراد است. ازآنجاکه امور زیست‌سنجی کاملاً به یک شخص وابسته هستند، باور بر این است که قابل اعتمادتر بوده، به سادگی فراموش، مفقود، دزدیده یا جعل نمی‌شوند و این از آن جهت است که شاخص زیست‌سنجی بر اطلاعات زیست‌شناختی منحصربه‌فردی از یک شخص مبتنی است. برای مثال، این اطلاعات می‌تواند تصویری سه بعدی از دست هر شخص، یک اسکن از عنبیه چشم شخص،

---

۱. این متن اقتباسی است از:

Paul, Rosenzweig. Alane Kochems, and Air Schwartz "Biometric Technologies: Security, Legal and Policy Implications", **Legal Memorandum**. No. 12, 2004.

2. Biometrics

۳. این مقاله مبتنی‌بر گزارش‌های ارائه‌شده پنجم مارس ۲۰۰۴ در میزگردی همنام با حامی مالی آن مرکز دموکراسی و فناوری و بنیاد هریتیج است. برای گزارش مبسوط درخصوص استفاده از فناوری زیست‌سنجی برای امنیت مرزی، رجوع کنید به:

Technology Assessment: Using Biometric for Border Security, GAO-03-174, Nov. 14, 2002.

4. See "Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism," Hearing before the Subcommittee on Technology, Terrorism and Government Information of the Senate Committee on the Judiciary, 107th Cong. Lst Sess, Nov. 14, 2001.

اثر انگشت یا ضبط صدای او باشد.

سیستم‌های زیست‌سنجی به دو منظور به‌کار می‌روند: احراز[1] یا تعیین هویت[2]. به هنگام استفاده از سیستم زیست‌سنجی برای احراز هویت مورد ادعای شخص، آن را تطابق «نفر به نفر» تعبیر می‌کنند. تقریباً تمام سیستم‌ها می‌توانند در کمتر از یک ثانیه تعیین کنند که آیا بین اطلاعات زیست‌سنجی ارائه‌شده و الگوی زیست‌سنجی در پایگاه داده‌ها تطابقی وجود دارد یا نه.

تعیین هویت بر خلاف مورد فوق به تطابق «فرد به جمع» معروف است. در تعیین هویت، اطلاعات زیست‌سنجی ارائه‌شده با تمام الگوهای زیست‌سنجی در پایگاه داده‌ها مقایسه می‌شود. دو نوع سیستم تعیین هویت وجود دارد: مثبت و منفی. انتظار می‌رود در سیستم‌های مثبت میان اطلاعات زیست‌سنجی ارائه‌شده و الگو تطابق وجود داشته باشد. این سیستم‌ها برای اطمینان دادن از وجود شخص در پایگاه داده‌ها و سیستم‌های منفی برای اطمینان دادن از عدم وجود او طراحی شده است. تعیین هویت منفی همچنین می‌تواند صورت یک فهرست نظارتی را به‌خود گیرد که در آن عمل تطابق، علامتی برای حکم مناسب یک اقدام ایجاد می‌کند.

هیچ‌کدام از سیستم‌های احراز و تعیین هویت تطابق کاملی ایجاد نمی‌کنند. در عوض، هریک از مقایسه‌ها درجه‌ای از کیفیت نزدیکی اطلاعات زیست‌سنجی ارائه‌شده را با الگوی ذخیره‌شده فراهم می‌آورد. سیستم‌های مذکور این درجه را با شماره‌ای ازپیش تعیین‌شده یا با الگوریتم‌هایی مورد مقایسه قرار می‌دهد و به‌این‌ترتیب مشخص می‌کند که آیا اطلاعات زیست‌سنجی موجود و الگو آنقدر به هم نزدیک هستند که یکسان تلقی شوند یا نه؟

اکثر سیستم‌های زیست‌سنجی به فرایند ثبت نام نیاز دارند که در آن نمونه‌ای از اطلاعات آنها به‌عنوان الگوی زیست‌سنجی ضبط، انتخاب و رمزگذاری می‌شود. سپس این الگو در پایگاه داده‌ها برای مقایسه‌هایی که در آینده صورت خواهد گرفت، ذخیره می‌شوند. هنگامی‌که سیستم زیست‌سنجی برای احراز (مثلاً نظارت بر دستیابی) مورد استفاده قرار می‌گیرد، این

1. Verification 2. Identification

سیستم اعتبار هویت ادعاشده را تأیید می‌کند. به هنگام استفاده از فناوری زیست‌سنجی برای تعیین هویت، این فناوری، اطلاعات زیست‌سنجی شخصی معین را با تمام رکوردهای ذخیره‌شده مقایسه می‌کند تا معلوم شود که آیا تطابقی وجود دارد یا خیر. پایگاه داده‌ها جهت کارایی بخشیدن به فناوری زیست‌سنجی، باید دقیق و نسبتاً گسترده باشد.

این فصل ابتدا بعضی از فناوری‌های مهمی را که درحال‌حاضر موجودند، ازجمله: شناسایی عنبیه، شکل دست‌ها، شناسایی انگشت، شناسایی صورت و تشخیص صدا ازطریق DNA مورد بررسی قرار می‌دهد و فایده عملی آنها را ارزیابی می‌کند. همچنین فناوری «تطابق با کارت» و «تست عملیات امنیتی و ایمنی اطلاعات مخاطره‌آمیز» را شرح می‌دهد که هر دو این فناوری‌ها به‌منظور فراهم آوردن امنیت بیشتر، فناوری‌های متعدد زیست‌سنجی را به‌صورت سیستمی واحد تلفیق می‌کنند. سپس پیامدهای سیاسی و قانونی استفاده از این فناوری را به‌منظور فراهم آوردن امنیت در جهان بعد از ۱۱ سپتامبر مورد بررسی قرار می‌دهد.

۲. کارایی و کارآمدی سیستم‌های زیست‌سنجی

به‌نظر می‌رسد فناوری‌های زیست‌سنجی ابزارهای مفیدی برای تعیین و احراز هویت در ابتکار عمل امنیتی باشند. امری که قبل از تحقق بخشیدن به این فناوری‌ها باید مورد توجه قرار بگیرد این است که آیا این سیستم‌ها واقعاً مؤثرند و آیا به‌منظور فراهم‌سازی قابلیت‌های بازاریابی و کارآمدی، به اندازه کافی پیشرفته هستند؟ دراین‌میان موضوعاتی از قبیل: اعتبار، امکان تقلب و رضایت مصرف‌کننده ملاحظات مهمی به‌شمار می‌روند. قابل ذکراست که این فناوری‌ها را به‌ویژه با ارزشی که دارند، به‌سختی می‌توان مورد مقایسه قرار داد.

۲ـ۱. فناوری شناسایی عنبیه

فناوری شناسایی عنبیه بر دایره رنگی مشخصی مردمک چشم را احاطه کرده است تکیه دارد. عنبیه تقریباً ۲۶۶ ویژگی مشخص دارد و شامل: شبکه غشایی، شیارها، حلقه‌ها، چین‌وچروک‌ها،

کرونای چشم[1] و لکه‌های آن می‌شود. معمولاً حدود ۱۷۳ ویژگی از این ویژگی‌های متمایز در ایجاد الگو به‌کار برده می‌شوند. عنبیه‌ها در طول هشتمین ماه حاملگی شکل می‌گیرند و باور بر این است که در طول مدت زندگی فرد ثابت باقی می‌مانند، مگر اینکه صدمه‌ای ببینند.

این سیستم‌ها معمولاً با استفاده از یک دوربین کوچک از عنبیه تصویری سیاه و سفید با کیفیت بالا می‌گیرند. سپس الگوریتم‌ها حدود عنبیه را مشخص و شبکه‌ای مختصاتی بر روی تصویر ایجاد می‌کنند. پس از آن، تمام ویژگی‌های انتخابی این بخش‌ها در پایگاه داده‌ها به‌عنوان الگوی زیست‌سنجی فردی ذخیره می‌شود.

هزینه هر واحد شناسایی عنبیه که معمولاً برای اجازه دسترسی فیزیکی به یک مکان مورد استفاده قرار می‌گیرد، در حدود دو هزار دلار برآورد می‌شود. این هزینه در مجموع سیستم گسترده تشخیص عنبیه خیلی بیشتر خواهد بود و شامل هزینه‌های سخت‌افزار، نرم‌افزار و جواز گرفتن می‌شود.

به‌کارگیری فناوری شناسایی عنبیه نسبتاً ساده بوده، می‌تواند افراد زیادی را به سرعت مورد بررسی قرار می‌دهد. همچنین این فناوری تنها میزان اندکی مزاحمت ایجاد می‌کند. باوجوداین لنزهای رنگی و دوکانونه چشم و نیز عینک‌های قوی ممکن است مانع کارایی سیستم شناسایی عنبیه شوند. نورهای قوی و انعکاس‌ها نیز می‌توانند برای دوربین‌ها مسئله‌ساز شوند. به‌علاوه آن دسته از کسانی‌که دید ضعیفی دارند، گاهی اوقات در تنظیم دقیق چشمانشان با دوربین‌ها دچار مشکل می‌شوند. سرانجام افرادی که به بیماری آب‌سیاه یا آب‌مروارید چشم مبتلا هستند، ممکن است نتوانند با اطمینان، از فناوری شناسایی عنبیه استفاده کنند.

۲ـ۲. شناسایی شکل دست‌ها

بررسی شکل دست‌ها بر میزان پهنا، بلندی و اندازه انگشت‌ها، فاصله میان مفصل‌ها و شکل

---

1. Corona

انگشت‌ها متکی است. با استفاده از دوربین‌های فوری و دیودهای نورپخش‌کن که دارای آینه‌ها و بازتابنده‌ها هستند، دو تصویر دوبعدی مستطیلی‌شکل از پشت و کناره‌های دست‌ها گرفته می‌شود. سپس براساس این تصویرها ۹۶ مقیاس مورد سنجش قرار گرفته، الگویی ایجاد می‌شود. بیشتر سنجش‌گرهای دست‌ها دارای گیره‌هایی هستند که به قرار گرفتن درست و ثابت آنها و تکرارپذیری الگو کمک می‌کنند؛ به‌گونه‌ای‌که دراین‌حالت میزان تشخیص‌های مثبت خطا و ناتوانی در انجام انطباق پایین است.

سیستم‌های سنجش‌گر شکل دست‌ها معمولاً ارزشی مابین دو تا چهار هزار دلار دارند. شناسایی شکل دست‌ها فناوری سنجیده‌ای است که بیشتر برای کنترل دستیابی و حضوروغیاب در حجم گسترده مورد استفاده قرار می‌گیرد؛ برای مثال، شرکت‌های کریسپی کرم[1] و مک دونالد[2] برای ثبت زمان حضوروغیاب کارکنان خویش به این فناوری متکی هستند. در مواقعی که افراد زیادی در زمانی بسیار کوتاه باید مورد بررسی قرار گیرند و نوع تطابق نیز باید نفر به نفر باشد، فناوری شکل دست‌ها کارایی خوبی دارد. اگرچه دست‌های افراد متفاوت هستند، به‌طور جداگانه متمایز نیستند. در نتیجه فناوری شناسایی شکل دست‌ها نمی‌تواند برای تطابق فردی به جمعی مورد استفاده قرار گیرد.

سیستم شناخت دست‌ها، سیستمی بسیار دقیق است که برای بیش از بیست سال در صنایع متنوعی برای تنظیم کنترل دستیابی از آن استفاده می‌شود. این سیستم در شناسایی اجازه ورود فرد به جایی یا انجام دادن امری نیز مفید است. این بسیار مشکل است که سایه دست کسی بدون همکاری او جعل شود. این اطلاعات ضروری به‌لحاظ فیزیکی برجای نمی‌ماند؛ برخلاف یک اثر انگشت که اغلب اینگونه است. بنابراین ساخت دستی بدلی که بدون اطلاع شخص مورد ثبت‌نام در دستگاه کارایی داشته باشد، بسیار مشکل است. این فناوری نسبتاً بادوام است (واحدهایی که در سال ۱۹۹۱ در این حیطه قرار داده شده است هنوز کار می‌کنند). بعد از

1. Krispy Kreme
2. Mc Donald

سال‌ها، تغییری اساسی در کاهش هزینه‌ها صورت گرفته است. دستیابی به بسیاری از مکان‌ها براساس سیستم شناخت دست‌ها استوار است؛ برای مثال، فرودگاه سان‌فرانسیسکو از آن برای دستیابی به پارکینگ فرودگاه استفاده می‌کند؛ بندر روتردام، پایگاه نیروی هوایی اسکاتلند و مجمع زنان[1] در دانشگاه اوکلاهما نیز بر این سیستم اتکا دارند.

اکثر مردم در استفاده از این فناوری راحت هستند. ازآنجاکه تصویری از یک دست نسبت به فناوری‌های دیگر مزاحمت کمتری ایجاد می‌کند، بیشتر افراد با ثبت‌نام در این برنامه موافقند. به‌علاوه این سیستم به‌لحاظ بهداشتی در حد گرفتن دستگیره یک در است. علاوه‌براین بی‌میلی مردم در قبول فناوری شناخت دست‌ها با دریافت این مسئله که آنها می‌توانند در عوض آن چیزی دریافت کنند، حل می‌شود. گولدز جیم[2] از واحدهایی برای دستیابی استفاده می‌کند که به اعضایش این امکان را می‌دهد تا از زحمت حمل کلید یا کارت خلاص شوند. دانشگاه جورجیا نیز از این فناوری برای تداوم برنامه وعده‌های غذایی استفاده می‌کند. این سیستم تقریباً در پانزده هزار دستگاه بانکی نیز به‌کار برده می‌شود.

۲ـ۳. شناسایی اثر انگشت

فناوری شناسایی اثر انگشت به‌طور گسترده‌ای بیشترین استفاده را دارد و از معروف‌ترین سیستم‌های زیست‌سنجی است. شناسایی اثر انگشت بر ویژگی‌هایی که در اثر ایجادشده از برجستگی‌های متمایز نوک انگشت یافت می‌شود مبتنی است. دو نوع اثر انگشت وجود دارد: صاف و گرد. اثر انگشت صاف، اثر قسمت مرکزی بند انگشت است؛ درحالی‌که اثر انگشت گرد، برجستگی‌های کناره‌های انگشت و بخش میان نوک انگشت تا اولین بند آن را ثبت می‌کند.

تصویرهای اثر انگشت اسکن و به‌لحاظ کیفی تقویت شده، سپس به الگوهایی تبدیل

---

1. Sorority
2. Gold's Gym

می‌شوند. این الگوها برای مقایسه‌هایی که در آینده با استفاده از اسکنرهای نوری، سیلیسیوم یا فراصوتی انجام می‌شود، در پایگاه داده‌ها ذخیره می‌شوند. اسکنرهای فراصوتی از بیشترین دقت برخوردارند؛ اما کمتر مورد استفاده قرار می‌گیرند. این اسکنرهای نوری‌اند که اغلب بیشترین استفاده را دارند.

به گزارش اداره کل حسابداری آمریکا سنجشگرهای اثر انگشت برای کنترل دسترسی فیزیکی بین یک تا سه هزار دلار هزینه دارند. همچنین هزینه اضافی مجوز نرم‌افزار در حدود چهار دلار برای هر کاربر برآورد می‌شود. هزینه نگهداری اسکنرهای کوچک انگشت‌نگاری نیز پانزده تا هجده درصد قیمت خریدشان است. اسکنرهای حضوری بزرگ‌تر، یعنی سنجشگرهای ده تصویری حدود ۲۵ هزار دلار قیمت دارند و هزینه نگهداری آنها حدود چهارده درصد قیمت خرید آنهاست.[1]

تنها درصد کمی از مردم نمی‌توانند در این سیستم ثبت شوند؛ به‌این‌دلیل که برجستگی‌های انگشت آنها از بین رفته، با کهولت سن صاف شده یا به‌علت استفاده از مواد شیمیایی فرساینده، سائیده شده است. علاوه‌براین افرادی هم هستند که استفاده از این فناوری را به‌دلیل ارتباط آن با انگشت‌نگاری قانونی به‌سادگی نمی‌پذیرند؛ برای مثال، فرهنگ‌های خاصی انگشت‌نگاری را با تعیین هویت به‌عنوان یک جرم یکسان نموده، از آن به‌عنوان سیستم زیست‌سنجی استفاده نمی‌کنند. همچنین این نگرانی وجود دارد که انگشت‌نگاری‌های انتخاب‌شده برای یک هدف، به‌منظور دنبال کردن فعالیت‌های شخصی در هرکجا که باشد نیز می‌تواند مورد استفاده قرار بگیرند. افراد گاهی از دست زدن به اسکنری که تعداد افراد زیادی آن را لمس کرده‌اند، با این تصور که غیربهداشتی است، شکایت می‌کنند. علاوه‌براین سیستم‌های زیست‌سنجی انگشت‌نگاری همه‌جا کارآمد نیستند؛ برای مثال، این سیستم در محیط‌هایی که از دستکش استفاده می‌شود، مثل اتاق

1. GAO, supra note 1, at 72.

عمل بیمارستان‌ها نامناسب است.

یکی از قسمت‌هایی که سیستم انگشت‌نگاری در آن مورد استفاده قرار می‌گیرد، بخش مدیریت بر تعیین هویت و دستیابی مراقبت‌های بهداشتی (مثل ادارات نظامی و بیمارستان‌های آموزشی) است. فناوری زیست‌سنجی برای حل این چالش که بیمارستان‌ها چطور به کاربرها می‌توانند امکان دسترسی دهند و درعین‌حال سطوح امنیتی لازم را برای آرامش و اطمینان فراهم نمایند، مورد استفاده قرار می‌گیرد. این چالشی خطیر است؛ زیرا تأمین امنیت بیشتر، دستیابی‌ها را کاهش می‌دهد. تعداد بسیار کمی اعتراض درباره این فناوری در بیمارستان‌ها وجود دارد. افراد به‌راحتی می‌پذیرند که اثرانگشت‌ها در پایگاه داده‌ها ذخیره شوند؛ زیرا بیشتر به‌صورت سلسله‌ای از اعداد ذخیره می‌شوند تا به‌صورت یک تصویر دیجیتالی واقعی.

۲ـ۴. شناسایی صورت

این فناوری شناسایی، صورت افراد را با تحلیل و ویژگی‌های خاص آن مثل: خطوط بالای حدقه چشم یا کناره‌های دهان شناسایی می‌کند. معمولاً سیستم شناسایی صورت، شخص حاضر را با الگوی ذخیره شده مقایسه می‌کند، اما این سیستم گاهی برای مقایسه میان تصویرهای ثابت و الگوها نیز استفاده می‌شود. این فناوری هم برای احراز و هم برای تعیین هویت به‌کار برده می‌شود. علاوه‌براین فناوری مذکور تنها فناوری سیستم زیست‌سنجی است که به‌طور معمول و مخفیانه برای انجام مراقبت مورد استفاده قرار می‌گیرد؛ زیرا صورت شخص به‌سادگی به‌وسیله فناوری ویدیویی ثبت می‌شود.

فناوری شناسایی صورت در عمل نقص بسیار کمی دارد. باوجوداین بنا به گزارش اداره کل حسابداری «به‌نظر می‌رسد عملکرد فناوری شناسایی صورت به فضای عملیاتی و کاربرد معین آنها بستگی دارد. آزمایش نظارت مبتنی‌بر شناسایی صورت در فرودگاه‌ها [نقص در میزان تطابق را] بین ۰/۳ تا ۵ درصد و [نقص در میزان عدم تطابق را] ۵ تا ۴۵ درصد ثبت کرده

است».[1] عوامل محیطی تأثیر مهمی بر روی این مقادیر دارند؛ زیرا هنگامی‌که تلاش می‌شود بین صورت ارائه‌شده و الگو تطابق انجام گیرد، نوسان در اجرای دوربین‌ها، موقعیت، حالت‌ها و خصوصیات صورت ممکن است مانعی برای الگوریتم‌ها باشند. قدمت الگو می‌تواند قابلیت یک انطباق صحیح را بیشتر تضعیف کند.

فناوری‌های شناسایی صورت می‌تواند بسیار گران باشد. «هزینه یک سرویس شناسایی صورت ناظر بر عملکرد در تأسیساتی با بیش از سی هزار نفر کاربر، در حدود پانزده هزار دلار است. بسته به تعداد ورودی‌های نصب‌شده در ابزارهای شناسایی صورت، هزینه مجوزهای نرم‌افزاری بین ۶۵۰ تا ۴۵۰۰ دلار در نوسان است».[2] هزینه سیستم با افزایش اندازه و تعداد تطابق‌های صورت‌گرفته افزایش می‌یابد. در مواردی که همراه با نرم‌افزار شناسایی صورت، تلویزیون‌های مدار بسته (CCTV) استفاده می‌شود، بسته به اندازه ورودی و نوع مانیتور مورد نیاز هزینه تلویزیون مداربسته از ده هزار تا بیست هزار دلار تغییر می‌کند. هزینه دوربین‌های اضافی تلویزیون مداربسته بین ۱۲۵ تا ۵۰۰ دلار در نوسان است که این هزینه برای دوربین‌هایی با ویژگی‌های پیشرفته تا سقف ۲۳۰۰ دلار افزایش می‌یابد.

---

۱. GAO, Supranote1, at 70. به هنگام ارزیابی فناوری‌های زیست‌سنجی سه ارزیابی مهم وجود دارد که شامل: میزان تطابق‌های اشتباه (FMR)، میزان عدم تطابق‌های اشتباه (FNMR) و ناتوانی در ثبت (FTER) است. تطابق اشتباه بدین معنی است که فناوری به اشتباه هویتی را با زیست‌سنجی ارائه‌شده تطابق داده و (FMR) عبارت از احتمال تطابق‌های غلط است. تطابق‌های اشتباه در یک سیستم تعیین هویتی مثبت بدین معناست که اشخاص غیرمجاز به منابع یا اماکنی که اجازه ندارند، دسترسی یابند. عدم تطابق‌های اشتباه (FNMR) هنگامی صورت می‌گیرد که فناوری مذکور یک زیست‌سنجی ارائه‌شده معتبر را رد می‌کند. عدم تطابق‌های اشتباه می‌تواند به‌معنای این باشد که یک شخص مجاز از دسترسی به اماکنی که واقعاً اجازه‌اش را دارد محروم گردد. (FTER) عبارت از احتمال این امر است که شخص قادر به ورود به پایگاه داده‌ها نباشد. این نقایص می‌توانند به دلایل مختلفی رخ دهند؛ ازجمله: ناتوانی در حصول یک نمونه به اندازه کافی متمایز یا سیستم‌هایی که مانع سنجش پیوسته هستند.

2. GAO, supra note 1, at 71.

۲ـ۵. تشخیص صدا

فناوری تشخیص صدا، افراد را براساس تفاوت‌های صوتی آنها شناسایی می‌کند که این تفاوت‌ها در نتیجه تفاوت‌های جسمی و عادات آموخته‌شده صحبت کردن به‌وجود می‌آید. به هنگام ثبت صدای فرد، این سیستم الگوهایی از گفتار شخص را با چند بار خواندن اطلاعات نوشته‌شده خاصی برای میکروفن و یا تلفن به ثبت می‌رساند. این اطلاعات به «عبارت عبور» معروف است (همچنین برخی سیستم‌های زیست‌سنجی موجود می‌توانند بدون نیاز به عبارت از پیش تعیین‌شده، صدای افراد را تشخیص دهند) سپس این عبارت عبور به طرحی دیجیتالی انتقال پیدا می‌کند و ویژگی‌های متمایز آن (مثل: زیروبمی، ریتم و آهنگ صدا) به‌منظور ایجاد الگویی برای گوینده انتخاب می‌شوند. الگوهای تشخیص صدا به بیشترین فضای اطلاعاتی در میان تمام الگوهای زیست‌سنجی نیاز دارند. فناوری تشخیص صدا برای هر دو هدف احراز و تعیین هویت قابل استفاده است.

این فناوری به حداقل آموزش برای کسانی‌که با آن کار می‌کنند، نیاز دارد و نیز نسبتاً ارزان و بدون هیچ‌گونه مزاحمتی است. فقط بزرگ‌ترین اشکال آن غیرقابل اعتماد بودنش است و اینکه در محیط‌های پرسروصدا (مثل محل‌های ورود) به‌خوبی کارایی ندارد.

برنامه دیدار از آمریکا نمونه‌ای از بخش‌هایی است که ممکن است در آن از سیستم تشخیص صدا استفاده شود؛ همچنان‌که یک شرکت این سیستم را در طرح خود آورده است. هر فردی که در کنسولگری آمریکا تقاضای ویزا کند، در پایگاه داده‌های تحت مدیریت آمریکا ثبت خواهد شد. هر شخص نام و پس از آن عبارت عبور خود را ثبت می‌کند. سپس کارکنان محلی، ایالتی و فدرال این کشور می‌توانند از تلفن موبایل یا یک سایت اینترنتی برای احراز هویت ادعاشده توسط فرد استفاده کنند. ازآنجاکه دارندگان ویزا یک‌بار به هنگام دریافت ویزایشان این روند را طی کرده‌اند، تکرار این مراحل در ایالات متحده برای آنها نباید خیلی مشکل باشد، هرچند به زبان انگلیسی صحبت نکنند.

۲ـ۶. شناسایی از طریق DNA

روش‌های فعلی شناسایی DNA به حداقل دویست یاخته که می‌توان از خون، منی یا پوست گرفت احتیاج دارد. یان فیندلی[1] و همکارانش در دانشگاه لیدز انگلستان درحال تحقیق درباره روشی هستند که فقط یک یاخته (مثلاً شوره‌سر) دراختیار دارد. در تکنیک آنها، شش بخش کروموزومی مختلف که الگوهای مولکولی‌شان به‌طورکلی در هر شخص یا شخص دیگر متفاوت است تجزیه‌وتحلیل می‌شود. پژوهشگران اشتباه مطابقت را یک در پنجاه میلیون گزارش می‌کنند.

روش دیگر آزمایش DNA که با استفاده از DNA میتوکندری انجام می‌گیرد، از ۱۹۹۶ به‌بعد مورد استفاده FBI قرار گرفته است. در روش آزمایش DNA میتوکندری می‌توان از موادی که بدون هسته، کوچک و کهنه‌تر هستند و به‌خوبی نگهداری نشده‌اند (مثلاً یک تار مو) استفاده کرد؛ اما عیبش این است که زیاد قابل اعتماد نیست. DNA میتوکندری، در فرزندان و مادر آنها و تمام اقوام مادری شخص یکسان است.

انگشت‌نگاری موروثی[2] ـ که به نام‌های «آزمایش DNA» یا «نمای DNA»، معروف است[3] ـ یکی از تکنیک‌هایی است که برای شناخت و تشخیص اشخاص مختلف، با نمونه‌برداری از DNA آنها انجام می‌گیرد. این شیوه توسط دکتر الک جفریس[4] در دانشگاه لیستر[5] در سال ۱۹۸۵ ابداع شد. تست ژنتیکی فرایندی است که در آن تغییرات رشته‌ها و خطوط DNA در حجم بالا مورد استفاده قرار می‌گیرد و در اصطلاح به آن «ماهواره‌های کوچک» می‌گویند. دو فرد غریبه ممکن نیست که خطوط مشابهی داشته باشند.

اثر ژنتیکی بیشتر در علم حقوق و قضا به‌کار می‌رود و برای تشخیص آن از گروه خون،

---

1. Ian Findly
2. Genetic Fingerprinting
۳. این متن اقتباسی از:
Genetic Fingerprinting:http://en.wikipedia.org/wiki/Genetic_fingerprinting
4. Alec Jeffreys
5. Leicester

رنگ مو، آب دهان یا منی مجرمان استفاده می‌شود. این روش همچنین برای اثبات بی‌گناهی یا سوءپیشینه نیز مورد استفاده قرار می‌گیرد و نیز در مواردی که درخواستی مبنی‌بر حضور فردی در جایی صورت می‌گیرد، انجام «تست پدری»، اهدای عضو، مطالعه بر روی گونه‌های مختلف حیوانات وحشی، تحقیق بر روی تولیدمثل و زندگی حیوانات یا فرضیه‌هایی مبنی‌بر چگونگی زندگی در ماقبل تاریخ نیز این علم کاربرد دارد.

این آزمایش، راه‌ورسمی قانونی در مسیر دادرسی و قضاوت است. این‌گونه آزمایش‌ها گاهی اوقات به‌صورت داوطلبانه توسط اشخاص صورت می‌گیرد که البته برای دادگاه یا سایر مراکز تحقیقاتی، معتبر نیست. بزرگ‌ترین مرکز نگهداری اطلاعات DNA در جهان، در آمریکاست[1] که در آن ۴/۵ میلیون اطلاعات DNA تا سال ۲۰۰۷ ثبت شده است. در انگلیس هم مرکز نگهداری اطلاعات ملی DNA (NDNAD) با تقریباً همین حجم اطلاعات فعالیت دارد.

۲ـ۶ـ۱. *منابع نمونه‌گیری*

تشخیص DNA باید با استخراج آن از بدن صورت گیرد، مانند:

- نمونه‌گیری وسایل شخصی (مانند: مسواک، ریش‌تراش و...)؛
- بانک اطلاعات و نمونه‌ها؛
- خویشان هم‌خون؛
- شناسایی وابستگان نسل‌های قبل.

۲ـ۶ـ۲. *روش‌های آزمایش DNA*

این آزمایش از نمونه‌گیری و ثبت اطلاعات مربوط به خون، بزاق، منی و ... به‌دست می‌آید.

۲ـ۶ـ۲ـ۱. *تحلیل RFLP*

یکی از روش‌های آزمایش DNA استفاده از لکه‌ها یا تکه‌های نمونه‌هاست که چند مرحله دارد: اول اینکه DNA ـ که در حال آزمایش است ـ باید از سایر مواد جدا باشد. بعد اینکه

1. The Combined DNA index system

باید به چند بخش مختلف تقسیم شود. سپس بخش‌های مختلف را طی عملیات «الکترو فورسیس»[1] (یا الکترون‌بری) مورد آزمایش قرار می‌دهند. این بخش‌ها را در ژل مخصوصی جاری کرده، موادی چون: دی‌اکسید کربن و... به آن می‌افزایند و نمونه‌های آنها را جذب می‌کنند. بخش‌های کوچک‌تر سریع‌تر در ژل حرکت کرده، حل شده، سپس به نسبت یکسان جدا می‌شوند. محلول قلیایی یا گرما بر روی ژل اثر داده شده و سپس لایه‌های «نیتروسلولوز»[2] روی آن فشار داده می‌شود و با گرما به خشک کردن آن می‌پردازند. در نهایت DNA پایدار از آن به‌دست می‌آید. اکنون DNA آماده تجزیه و تحلیل است و توسط اشعه رادیواکتیو بررسی می‌شود.

برای ساخت الکترود رادیواکتیو به پلیمرهای DNA نیاز است. DNAهایی که جهت ساخت رادیواکتیو انتخاب می‌شوند، باید در لوله‌ای ریخته شوند. برش‌های افقی باید در طول آنها ایجاد و در همان زمان نیز نوکلئوتیدها باید افزوده شود. هسته C یا سایتوسین[3] رادیواکتیو است. سپس پلیمرها باید به لوله اضافه شوند. آنها جذب خواهند شد و قطعات شکسته را ترمیم می‌کنند. وقتی که پلیمرهای DNA ترمیم شدند، پیوند یونی بین آنها شکسته و نوکلئوتیدهای موجود، جایگزین نوکلئوتیدهای قبل می‌شوند. هنگامی‌که رشته‌های زیرین به هسته G برسند، یعنی به گوانین C5H5N5O تبدیل شوند، هسته C در داخل آن، واکنش ر دیواکتیوی خواهد داد. با بازسازی رشته‌های DNA پلیمرها خاصیت رادیواکتیوی پیدا می‌کنند. در این مرحله DNAها چنان داغ می‌شوند که دو رشته از آنها شکافته می‌شود. رشته‌های مجزای دیگری که ممکن است رادیواکتیو باشند یا نباشند نیز در این مرحله ساخته می‌شوند. بخش‌های رادیواکتیو در این مرحله برای استفاده بررسی می‌گردند. این واکنش ر دیواکتیوی باعث ایجاد واکنش پیوندی می‌شود. برای تشکیل این واکنش پیوندی، DNA به رشته‌های مستقل تغییر ماهیت می‌دهد. این رشته‌ها و اشعه رادیواکتیو باید در ظرفی پلاستیکی ریخته شده، آب پرنمکی به آن اضافه و خوب تکان داده شود. اشعه رادیواکتیوی با DNAهای

1. Electro phoresis
2. Nitrocellulose
3. Cytosine

تغییر ماهیت داده ترکیب و آماده می‌شود. الکترودهایی که دارای همتایی پایینی هستند یا مشابهند، بهتر می‌توانند با DNA پیوند داشته باشند. اگر پیوند اتفاق نیفتد، الکترود و DNA پیوند دورگه تشکیل می‌دهند و راه استفاده از آن، مشخص کردن VNTR شخصی است. VNTR یعنی تعیین تعداد رشته‌های تکراری تغییرپذیر که در ژن وجود دارد. هر رشته از DNA دارای شکافی است که در آن اطلاعات مربوط به ژن قرار دارد و به آن اکسون[1] می‌گویند. هر فردی به‌طور مخصوص، این اطلاعات ژنتیکی را در رشته‌های DNA خود دارد و نقوش VNTR نیز در هر فردی منحصر به خود او و بسیار دقیق است.

۲ـ۶ـ۲ـ۲. تجزیه PCR

با اختراع PCR (واکنش زنجیره پلیمری)، آزمایش تشخیصی DNA گام بلندی به‌سوی جلو برداشت. این پیشرفت در هر دو مورد کاربرد DNA، یعنی قدرت تشخیص و توان بازیافت اطلاعات از رشته‌های کوچک کارایی دارد. PCR دامنه و گستره DNA را در خود می‌پیچد و چرخه‌ای حرارتی و مقاوم در برابر گرما تشکیل می‌دهد. کیسه‌های صنعتی که برای نگهداری از این مواد استفاده می‌شوند SNP نام دارند و به تقویت PCR نیز کمک می‌کنند.

یکی از ایرادات اصلی که بر RFLP گرفته می‌شود، این است که بسیار وقت‌گیر است و به چندین رشته DNA جهت انجام مراحل آزمایش نیاز دارد؛ ولی روش PCR در مقایسه با آن سریع‌تر بوده، مقدار کمتری DNA نیاز دارد. همچنین در روش RFLP شرح ساختار DNA نیز مشکل است؛ مثلاً در این روش تعیین DNA فردی که تجاوز به عنف کرده، از راه آزمایش‌های واژینال کار ساده‌ای نیست.

۲ـ۶ـ۲ـ۳. اندازه‌گیری FLP

یکی دیگر از تکنیک‌های موجود، اندازه‌گیری FLP[2] است که از ابتدای دهه نود مورد توجه و آزمایش قرار گرفت. این تکنیک از تجزیه RFLP بسیار سریع‌تر است و بر روی شمار

---

1. Exon
2. Amplified Fragment pholymorphism

زیادی از رشته‌های VNTR برای یافتن اطلاعات کاربرد دارد. در این روش که از ژل «پلی اکریلامید»[1] استفاده می‌شود، قابلیت کار کردن به‌صورت اتوماتیک نیز وجود دارد؛ به‌همین‌دلیل از آن در قوانین و مقررات مالی بسیاری از کشورها استفاده می‌شود.

۲-۶-۲-۴. تجزیه STR

امروزه رایج‌ترین روش تست وراثتی که براساس PCR انجام می‌شود STR[2] است. در این روش از قسمت‌های پلی‌مورفیک (چند شکلی)[3] نمونه DNA جهت آزمایش استفاده می‌شود؛ زیرا مردم مختلف در مقدار رشته‌های DNA متفاوت هستند. این قسمت از DNA می‌تواند برای تمایز و تشخیص صفات ارثی در مردم مختلف مورد استفاده قرار گیرد. این ناحیه (محل استقرار STR) با آستری از مواد PCR پوشیده شده، تقویت می‌گردد و تکه‌های مختلفی از DNA به‌وجود می‌آید که این تکه‌ها جدا شده و توسط فرایندی شیمیایی، الکترون‌بری می‌شوند. اینک دو روش مشابه برای جداسازی وجود دارد: الکترون‌بری مویینه‌ای[4] و الکترون‌بری با ژل[5].

آشکار کردن چندگونه‌ای در هر ناحیه STR مشابه است. انواع گونه‌های زیستی انسانی، معمولاً به پنج بخش تقسیم می‌شوند و وقتی به جایگاه چندلایه‌ای آنها دقت گردد، یک دسته ترکیبی از این چندگونه‌ای مشاهده می‌شود.

در کشورهای مختلف، اجرای آزمایش STR از روی DNA متفاوت است. در شمال آمریکا این سیستم که با CODIS 13 تقویت می‌شود و در محل درونی DNA آزمایش انجام می‌گیرد، تقریباً شیوه‌ای جهانی است. در انگلستان سیستم +SGM که با مرکز اطلاعات DNA نیز سازگار است استفاده می‌شود. هر کدام از سیستم‌ها که به‌کار می‌رود، اطلاعات مشابهی را به‌دست می‌دهد. الکترون‌بری مویینه‌ای یا نازک به‌وسیله برق جنبشی[6] کار می‌کند. تزریق

---

1. Polyacrylamide
2. Short Tandem Repeat
3. Polymorphic
4. Capillary Electrophoresis
5. Gel Electrophoresis
6. Electro kinetically

تکه‌های DNA در یک لوله نازک شیشه‌ای که از پلیمر پر شده است، انجام می‌شود. DNA در اطراف لوله شیشه‌ای پخش شده و جریان الکتریکی بر روی آن توسط یک قطب الکتریکی گسترده می‌شود. تکه‌های مختلف DNA به‌خصوص تکه‌های کوچک‌تر، شروع به حرکت سریع در لوله شیشه‌ای می‌کنند. تکه‌های کشف شده DNA در رنگین نمودن فلورسنتی مورد استفاده قرار می‌گیرند که این ماده رنگین جهت آستری کردن در PCR به‌کار می‌رود. این قضیه سبب می‌شود که تکه‌های چندلایه DNA تقویت شده، جهش همزمان داشته باشند. این شیوه البته بسیار هزینه‌بردار است و ابزارآلات سنگینی را نیز نیاز دارد.

مدل کاربری روش یون‌بری با ژل نیز همانند الکترون‌بری مویینه‌ای است؛ فقط با این تفاوت که به‌جای استفاده از شیشه نازک، ژل پلی‌اکریلامید برای جدا کردن تکه‌های DNA مورد استفاده قرار می‌گیرد. یک قطب الکتریکی نیز همان‌طور که در روش شیشه نازک بود وجود دارد. باز هم با ورود جریان برق تکه‌ها حرکت می‌کنند و تکه‌های ریزتر سریع‌ترند. میدان حرکت آنها در محفظه ژلی است. تمام بخش‌های ژل (اعم از خالص و دست‌خورده) در کامپیوتر مورد بازدید قرار می‌گیرند. بدین‌ترتیب تصویری به‌وجود می‌آید که تمام رشته‌های مطابق با تفاوت‌های ژنی را نشان می‌دهد. در این روش سایز استاندارد برای رشته‌ها وجود ندارد. اهمیت روش تجزیه STR در قدرت دسته‌بندی آماری آن است.

احتمال تفاوت گونه‌ای می‌تواند بسیار متفاوت باشد. در عوض پس از زادوولد سیزده نسل ممکن است یک در یک کوین تیلیون[1] (یعنی یک با هجده صفر جلوی آن) شباهت ژنتیکی وجود داشته باشد.

۲ـ۶ـ۲ـ۵. تجزیه Y کروموزوم[2]

نوآوری‌های اخیر محملی برای ایجاد نواحی اصلی چندگانگی زیستی است. Y کروموزم (Y-STR) باعث جدایی لایه‌های نرینه می‌گردد. این کروموزوم‌ها الگوهای وراثت هستند؛

---

1. Quintilion 2. Ychromosome

بنابراین تجزیه آنها باعث کشف مسائل جدید شده، به شناخت الگوهای وراثتی نرینه کمک‌های بسیاری می‌کند. تجزیه YSTR توسط نظرها و عقاید سالی همینگز[1] به‌وجود آمد.

۲ـ۶ـ۲ـ۶. آنالیز میتوکندریال[2]

در نمونه‌های خفیف‌شده کروموزوم‌ها گاهی به‌دست آوردن اطلاعات جامع و کامل از CODIS 13 STRها غیرممکن است. در این مواقع، میتوکندریال DNA می‌تواند راه‌حل مناسبی باشد. با تقویت دو رشته از هسته DNA می‌توان به اطلاعاتی دست یافت. با تقویت نواحی HV1 و HV2 در میتوکندریال DNA این عمل شدنی خواهد بود؛ زیرا میتوکندریال DNA دارای صفات ارثی است و این صفات می‌توانند اطلاعات زیادی از صفات ارثی خانوادگی را به‌دست دهند؛ مانند پسر خواهر مادر بزرگ مادری. تفاوت در دو یا چند نوکلئوتید معمولاً مورد بررسی قرار می‌گیرد. میتوکندریال DNA در مشخص کردن و شناسایی هسته اصلی رشته‌های اطلاعاتی کاربرد دارد؛ مانند افراد ناشناسی که از روی صفات وراثتی از ناحیه مادری خود شناسایی می‌شوند. این آزمایش نشان داد که «آنا اندرسون»[3] یک شاهزاده روسی نیست. نمونه‌های دیگر این آزمایش را می‌توان با تارهای مو یا استخوان‌ها و دندان‌های کهنه انجام داد.

۲ـ۶ـ۳. ملاحظات لازم در بررسی *DNA*

در مواقعی که از تست ژنتیک برای اثبات مسائل جنایی و حقوقی استفاده می‌شد، هیئت منصفه در صدور رأی مردد بود. آنها معتقد بودند این مسئله جنبه علمی ندارد و احتمال می‌دادند در هر پنج میلیون نفر، یک نفر از این مسئله مستثنی بوده، جواب آزمایش وی درست نباشد. وکلا و مشاوران حقوقی استدلال می‌کردند که در یک کشور شصت میلیونی، دوازده نفر وجود دارند که تست ژنتیکی آنها با هم مشابه است. همچنین برخی مشاوران حقوقی ریسک استفاده از

---

1. Sall Hemings
2. Mitochondrial
3. Anna Anderson

آزمایش RFLP را یک در صد میلیارد[1] می‌دانستند. باوجوداین میزان خطای آزمایشگاهی مسلماً بیشتر از این مقدار است؛ برای مثال، احتمال شباهت (خطای آزمایشگاهی) ممکن است براساس نشانه‌هایی که در رشته‌های مختلف است به‌وجود آید؛ ولی مسئول آزمایشگاه وظیفه دارد این نشانه‌های ریز را به‌دقت بررسی کند.

امروزه استفاده از RFLP به‌دلیل افزایش آمار قضاوت اشتباه به‌طور جدی کنار گذارده شده است؛ ولی STR از چنین قاعده‌ای مستثنی بود. آماری که انگلیس از این آزمایش ارائه می‌دهد، نشان از قدرت تشخیص دقیق‌تر این آزمایش دارد و البته میزان احتمال اشتباه در آن، یک در ۱۰,۰۰۰,۰۰۰,۰۰۰,۰۰۰ است و در این روش، استفاده از آزمایش SGM نیز لازم است.

شایان ذکر است که هیچ‌یک از تکنیک‌های تست DNA همواره دقیق نیستند و دادگاه‌ها نباید فقط با استناد به آزمایش DNA رأی دهند، بلکه باید سایر مدارک و شواهد را نیز بسنجند.

در حقیقت وقتی تست DNA بررسی می‌شود، سؤالات زیر باید پرسیده شود:

- آیا این تست می‌تواند به‌طور تصادفی شبیه دیگری داشته باشد؟
- اگر نه، آیا ممکن است رشته‌هایی از DNA پنهان شده باشد؟
- اگر نه، آیا آزمایش DNA در زمان مناسبی از محکومیت گرفته شده است؟
- اگر بله، آیا این آزمایش گناهکار بودن متهم را اثبات می‌کند؟

۲ـ۶ـ۴. DNA قلابی

ارزش تست DNA به شفافیت آزمایش و عدم کاشت DNA قلابی است. در یکی از موارد، متهم به کاشت DNA قلابی در بدن خویش پرداخته بود. دکتر «جان اشنیبرگر»[2] از کانادا، به یکی از بیمارانش تجاوز جنسی کرد (در سال ۱۹۹۲). پس از دستگیری، از وی آزمایش DNA

---

۱. ۱۰۰ میلیارد = ۱۰۰,۰۰۰,۰۰۰,۰۰۰

2. John Schneeberger

به‌عمل آمد؛ ولی جواب آن با تست DNA منی که از وی خارج شده بود مطابقت نداشت. بعد مشخص شد که او در زیر پوست بازوی خود داروی «پن روس»[1] قرار داده و باعث بروز اطلاعات غلط در خون شده است.

۲ـ۶ـ۵. برخی نمونه‌ها از تست DNA

در سال ۱۹۲۰ «آنا اندرسون» مدعی شد که شاهزاده‌ای از تبار «رومانوف»[2] (از تزارهای روسیه) است. در سال ۱۹۸۰ وقتی که وی مرد، از رشته‌های دستمال او که در «شارلوتسویل»[3] نگهداری می‌شد آزمایش DNA کردند و فهمیدند که وی هیچ نسبتی با «رومانوف‌ها» ندارد.

در سال ۱۹۸۷ یک نانوای انگلیسی به‌نام «کلین پیچفورک»[4] اولین کسی بود که از وی آزمایش DNA جهت رأی دادگاه به‌عمل آمد. وی در شهر «لیستر»[5] ـ اولین شهری که این آزمایش در آن انجام شد ـ زندگی می‌کرد.

در سال ۱۹۸۷ یک متجاوز فلوریدایی[6] به نام «تامی لی»[7] اولین کسی بود که در آمریکا توسط جواب آزمایش DNA محکوم شد. وی به جرم تجاوز به یک زن از راه ورود غیرقانونی به منزل او، در تاریخ ۶ نوامبر ۱۹۸۷ به ۲۲ سال زندان محکوم شد.

در سال ۱۹۸۸ «تیموتی سپنسر»[8] اولین مردی بود که در آمریکا به جرم چندین فقره قتل و زنا، به استناد آزمایش DNA محکوم به مرگ گردید.

در سال ۱۹۸۹ مردی از اهالی شیکاگو به نام «گری دستون»[9] اولین کسی بود که به‌واسطه آزمایش مذکور تبرئه شد.

در سال ۱۹۹۱ «آلان لگر»[10] اولین فرد کانادایی بود که به جرم چهار قتل محکوم شد و آزمایش DNA وی نیز این مسئله را تأیید کرد.

---

1. Penrose
2. Romanov
3. Charlottesvill
4. Colin Pitchfork
5. Leicester
6. Florida
7. Tommie lee
8. Timothy Spencer
9. Gary Doston
10. Allan Legere

در سال ۱۹۹۲ به استناد آزمایش DNA مشخص گردید که دکتر «ژوزف منگل»[1] در برزیل، با نام «ولفگانگ گرهارد»[2] دفن شده است.

در سال ۱۹۹۳ «کیرک بلود بلاذروورث»[3] اولین شخصی بود که گرچه متهم به قتل و محکوم به اعدام بود، محکومیتش با استفاده از تست DNA لغو شد.

در سال ۱۹۹۴ آزمایش RCMP بر روی موی یک گربه و نیز مردی که همسر خود را به قتل رسانده بود انجام شد، و این‌گونه برای اولین بار آزمایش DNA بر روی حیوان و سپس انسان‌ها صورت گرفت.

۲ـ۷. فناوری زیست‌سنجی تطابق با کارت

فناوری تطابق با کارت تقریباً با هر سیستم زیست‌سنجی، قابل استفاده و معمولاً به شکل کارت‌های هوشمند است. این کارت‌ها دارای الگوهای زیست‌سنجی (مثل: اثر انگشت دیجیتالی و رمزگذاری شده) ذخیره شده در تراشه‌ای کامپیوتری هستند. نسخه موجود از اثر انگشت با الگوی ذخیره‌شده به‌منظور احراز هویت مقایسه می‌شود. مزیت این فناوری این است که می‌تواند به‌عنوان بخشی از شبکه‌ای به‌کار رود که در آن شبکه اطلاعات زیست‌سنجی ارائه‌شده با پایگاه داده‌های تمرکزیافته یا محلی مقایسه می‌گردد و یا برای مقایسه‌ای میان اطلاعات زیست‌سنجی ارائه شده و الگوی موجود بر روی خود کارت، مورد استفاده قرار می‌گیرد. کارت‌های هوشمند دراصل به‌عنوان «عامل امنیتی سازمان صادرکننده در دستان کاربر» عمل می‌کنند. علاوه‌براین سطوح امنیتی موجود قابل درجه‌بندی هستند. فرد می‌تواند این کارت را به همراه اطلاعات زیست‌سنجی یا با شماره شناسایی شخصی مورد استفاده قرار دهد، یا اینکه کارت‌ها را همراه با الگوهای زیست‌سنجی مورد استفاده در ترکیب با شماره شناسایی

---

1. Joseph Mengel
2. Wolfgang Gerhard
3. Krik Bloodsworth

شخصی به‌کار برد. سیستم پاسپورت‌های پیشنهادی الکترونیکی[1] که اکنون در سطح جهانی در حال گسترش هستند، فرمی از فناوری تطابق با کارت به‌شمار می‌روند.[2]

۲ـ۸. زیست‌سنجی برای امنیت حمل‌ونقل مواد خطرناک

این شیوه فناوری‌های زیست‌سنجی را برای تأیید راننده مورد استفاده قرار می‌دهد. کارت‌های هوشمند و فناوری‌های زیست‌سنجی در تأیید هویت رانندگان نزد فرستندگان، دریافت‌کنندگان و خودروهای رانندگان مورد استفاده قرار می‌گیرند. این کارت‌ها که حاوی اطلاعات از پیش تعیین‌شده خاص راننده هستند، همراه با اسکنرهای انگشت برای تأیید هویت رانندگان استفاده می‌شوند. این فناوری‌ها همچنین رویداهای مربوط به کاهش، شتاب و آغاز به کار کامیون را ثبت می‌نمایند. این معرفی زیستی (بیولوگین) در کامیون به ارسال‌کنندگان درصورتی‌که شخص غیرمجازی سعی در روشن کردن کامیون داشته باشد هشدار می‌دهند. فناوری‌های زیست‌سنجی و کارت هوشمند همچنین برای تأمین امنیت سیستم بارنامه حمل مورد استفاده قرار می‌گیرند؛ به‌گونه‌ای‌که تنها استفاده‌کنندگان مجاز برای ارسال بارهای خطرناک بتوانند اسناد را صادر یا بازرسی کنند یا بتوانند خودشان به بارها دسترسی داشته باشند.

دراین‌راستا بزرگ‌ترین مشکل به بی‌حوصلگی راننده درخصوص برخی رویه‌های اثباتی متکی بر اطلاعات انتقالی ماهواره که طی مواقع سنگینی بار می‌تواند کند باشد، مربوط بوده است.

۲ـ۹. فناوری‌های درحال ظهور

علاوه بر فناوری‌های تکامل‌یافته مورد بحث در بالا، محققان در جستجوی زیست‌سنجی‌های

---

1. E-Passport
2. See Ha Nguyen, Paul Rosenzweig & James Jay Carafno, "E-Passports: A Strategy for Long-Term success", **Heritage Foundation Executive Memorandum**, No. 921, April 13, 2004.

مفید دیگری نیز هستند. برخی از این فناوری‌های درحال ظهور عبارتند از: بررسی دقیق سیاهرگ‌ها، گرمانگاری (ترموگرافی) صورت، تطابق DNA، احساس بو، مقیاس‌های فشار خون، و تشخیص الگوی پوست، بافت ناخن، طرز راه رفتن و شکل گوش‌ها. برخی از این فناوری‌های زیست‌سنجی، مانند: بررسی دقیق سیاهرگ‌ها به‌تازگی در بازار موجود می‌شوند. برخی موارد دیگر نیز از قبیل: تشخیص شکل گوش پروژه‌های تحقیقاتی هستند که به‌تازگی شروع شده‌اند.

هر سازمان علاقه‌مند به حفاظت زیست‌سنجی باید به‌دقت مطالبات خویش را درنظر گیرد و آنگاه آن نوع فناوری زیست‌سنجی و حفاظتی مربوطه را که آن مطالبات را برآورده می‌سازند برگزینند. سازمان باید سطح امنیتی را براساس میزان تهدید انتخاب کند. هر چه امنیت بیشتری برای بازداری افراد از گول زدن سیستم مورد استفاده قرار گیرد، امکان پاسخ‌های مثبت بیشتر خواهد شد؛ به‌عنوان نمونه، اگر سازمانی بخواهد از یک فناوری زیست‌سنجی برای زمان و پذیرش استفاده کند، احتمال ندارد به این مسئله اهمیت دهد که آیا نمونه مورد نظر زنده است یا خیر؛ تهدید موجود برای چنین حفاظت‌های امنیتی بسیار کم است.

۳. نتایج قانونی و سیاسی

طبق بررسی فوق، استفاده از فناوری‌های زیست‌سنجی بسیاری سؤالات سیاسی متداخل را مطرح می‌کند که برخی از آنها در مورد تمامی سیستم‌های زیست‌سنجی مصداق کلی دارند و برخی دیگر مختص فناوری یا استفاده از آن هستند. از بین سؤالات قابل پرسش می‌توان اشاره کرد به اینکه: آیا سیستم زیست‌سنجی می‌تواند به‌دقت برای کار خویش تناسب یابد؟ چه کسی بر برنامه نظارت خواهد کرد؟ چه جایگزین‌های دیگری برای فناوری‌های زیست‌سنجی وجود دارند؟ چه اطلاعاتی ذخیره خواهند شد و به چه شکلی؟ فناوری زیست‌سنجی به چه قابلیت‌ها یا موقعیت‌هایی امکان دسترسی می‌دهد؟ آیا مواد زیست‌سنجی اصلی حفظ خواهند شد؟ آیا اطلاعات از دیگر اطلاعات شخصی تعیین هویت جدا نگه داشته خواهند شد؟ چه کسی به این

اطلاعات دسترسی خواهد داشت؟ دسترسی به اطلاعات چگونه کنترل خواهد شد؟ سیستم صحت اطلاعات را چگونه تضمین می‌کند؟ آیا اطلاعات در پایگاه‌های اطلاعاتی تلفیق خواهند شد؟ اگر اطلاعات در یک پایگاه اطلاعاتی ذخیره می‌شود، چگونه از آن حفاظت خواهد شد؟ چه کسی اطمینان می‌دهد که اداره‌کنندگان برنامه نسبت به نگرانی‌های مربوط به حریم خصوصی افراد پاسخگو خواهند بود؟ آیا افراد می‌توانند داوطلبانه از یک پایگاه اطلاعات خود را خارج سازند (خود قادر به «لغو ثبت نام» هستند؟) هماهنگی اطلاعات جمع‌آوری‌شده در محل‌های چندگانه چگونه حفظ می‌گردد؟ اگر انتخابی وجود دارد، آیا به افراد درخصوص راه‌های انتخابی در برابر راه‌های الزامی اطلاع داده خواهد شد؟

پاسخگویی به این پرسش‌ها دشوار است؛ بااین‌حال ما مطالب مقدماتی زیر را به‌عنوان چارچوبی برای پاسخگویی به آنها پیشنهاد می‌کنیم:

نخست، سودمندی تعیین هویت زیست‌سنجی به‌عنوان موضوعی کلی قابل قبول است. فناوری‌های زیست‌سنجی قابلیتی اساسی در بهبود امنیت ملی ازطریق تدارک ابزاری برای تعیین و احراز هویت افراد در بسیاری از موقعیت‌ها دارند. در بسیاری موارد آنها فراتر از ابزارهای رایج تعیین هویت امنیتی را فراهم می‌آورند. این امر در کنترل دسترسی به محل‌هایی که خطرهای امنیتی در آنها به‌طور ویژه‌ای بالاست (مانند: پارکینگ هواپیماهای فرودگاه، تجهیزات تأسیسات زیربنایی حاد، و مواردی از این قبیل) سودمندی خاصی خواهد داشت.

از این فناوری همچون هر فناوری جدید دیگری می‌توان سوءاستفاده کرد. بنابراین نگرانی عمومی به حقی وجود دارد درخصوص‌اینکه فناوری زیست‌سنجی ممکن است برای دخالت یا نقض حریم خصوصی شخصی یا دیگر آزادی‌های مدنی مورد سوءاستفاده قرار گیرد. برخی از ترس‌های مربوط به اطلاعات زیست‌سنجی عبارتند از اینکه این اطلاعات بدون اجازه، اطلاع یا دلایل تعریف‌شده روشن جمع‌آوری شوند؛ برای مجموعه‌ای از اهدافی غیر از آنچه در ابتدا برای آن جمع‌آوری شده‌اند مورد استفاده قرار گیرند؛ بدون اجازه‌ای صریح منتشر گردند؛ برای کمک به ایجاد تصویر کاملی از افراد جهت مراقبت یا اهداف مربوط به کنترل اجتماعی مورد

استفاده قرار گیرند. همچنین نگرانی‌هایی درخصوص ردیابی وجود دارد که عبارت است از: نظارت فوری یا تقریباً فوری یک فرد و نیز نگرانی‌هایی در مورد شرح‌حال‌نویسی که در آن فعالیت‌های گذشته شخص بازسازی می‌شوند؛ هر دوی اینها ناشناختگی وی را خراب می‌کنند.[1] همچنین نگرانی‌هایی در مورد جعل هویت نیز وجود دارد.

در پرتو این ترس‌ها و ترس‌هایی مشابه، برخی نتیجه‌گیری می‌کنند که این فناوری اصلاً نباید گسترش یابد؛ اما با درنظر گرفتن تهدید جدی‌ای که ما با آن مواجه هستیم، اگر ثابت شده است که فناوری زیست‌سنجی در زمینه‌های خاصی امنیت را افزایش می‌دهد و حفاظت‌های مناسبی را می‌تواند فراهم کند، می‌توان متقاعد شد که این امر ارزش پی‌گیری را دارد.

برخی از منتقدان زیست‌سنجی معتقدند که آزادی از ناشناختگی[2] ناشی می‌شود؛ درحالی‌که طرفداران آن این دیدگاه را دارند که امنیت مناسب وابسته به تعیین هویت کامل است و آزادی به هیچ‌وجه در خطر نخواهد بود.[3] بااین‌حال، به‌جای وابستگی صرف به ناشناختگی یا تعیین هویت کامل، دامنه‌ای از راه‌حل‌های تأییدکننده که متناسب زمینه تعامل بین دولت و فرد باشند مناسب‌تر به‌نظر می‌رسد.

توجه به این امر اهمیت دارد که بین ناشناختگی کامل و تعیین هویت کامل درجه‌بندی‌هایی وجود دارد. بسیاری از تعاملات با دولت می‌توانند بدون نیاز به اطلاعات شخصی مفصل تحقق یابند، هرچندکه این موارد کاملاً ناشناخته (گمنام) نخواهند بود. درواقع ما پیشاپیش، فهمی درجه‌بندی‌شده از تعیین هویت را آغاز کرده‌ایم؛ طیفی از راه‌حل‌های تأیید و تعیین هویت

---

1. See for instance: Jay Stanley & Barry Steinhardt, **Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society**, Washington, D.C: ACLU Technology and Liberty Program, 2003.

۲. رجوع کنید به Phillip Kurland, "The private I," **The University of Chicago Magazine,** Autumn 1976, p.8 (سه جنبه حریم خصوصی به‌طور گسترده در قالب ناشناختگی، محرمانه بودن و استقلال شخصی توصیف شده‌اند.) quoted in Whalen V. Roe, 429 U.S. 589-599, No. 24 1977.

3. See Alan Dershowitz "Why Fear National ID Cards?" **The New York Times,** Op-Ed, October 18, 2001.

شخصی در دسترسی دولت قرار دارد.[1] در تعاملی که هیچ اطلاعاتی در مورد هویت فردی لازم نیست، اما تأیید واقعی مورد نیاز است؛ به‌عنوان مثال برای استفاده در یک مطالعه تحقیقاتی دولتی جاری، سطح پایین‌تری از تأیید مورد نیاز خواهد بود. برخلاف این، در مواردی که هویت واقعی مهم نیست، اما به اطلاعات مربوط به تعیین هویت نیاز است (مثلاً برای دریافت بایگانی‌ها حین کار از یک شرکت) سطحی بالاتر باید وجود داشته باشد.

آنچه این مثال‌ها نشان می‌دهند، چندان مربوط به این نیست که مفهوم ما از آزادی، مبتنی‌بر انتظارات خصوصی مطلق است، بلکه بیشتر نشانگر این است که هرگونه تأثیرگذاری دولت بر آزادی ما تنها با دلایلی کافی صورت خواهد گرفت.[2] ما باید قادر به بیان دیدگاه‌های سیاسی بحث‌انگیز باشیم، با این انتظار که دولت فقط آن مواردی را مورد تحقیق قرار می‌دهد که واقعاً ممکن است منافع ملی را تهدید کنند. هنگامی‌که یک تحقیق جنایی یا تروریستی درحال انجام است، می‌توانیم انتظار داشته باشیم که کانون توجه بررسی‌ها، بدون دلیل کافی معطوف به فرد فرد ما نباشد. باوجوداین بیشتر تعاملات با دولت در حدی بین انتظار ناشناختگی کامل و بررسی مفصل قرار می‌گیرند. ما می‌توانیم همچنان انتظار داشته باشیم که دولت اطمینان خواهد داد که هرگونه تأثیرگذاری ممکن بر آزادی متناسب با تعامل با افراد است و اینکه دولت ابزارهای تکنولوژیک جهت دستیابی به این امر را داراست. اگر هیچ طیف واقعی از گزینه‌های تأیید هویت برای استفاده (از ناشناختگی گرفته تا برخورداری از نام مستعار و تعیین هویت کامل) وجود ندارد، تمامی انتظارات مربوط به حریم خصوصی تضعیف خواهند شد و آن هم صرفاً بدین‌علت که دولت مجبور است با هرگونه تعاملی، همچون موردی تحقیقی برخورد کند.

در بسیاری موارد، اجرای قوانین و سیستم‌های جدید جهت مبارزه با ترور عبارت از تقلیل صرف حریم خصوصی افراد نیست، بلکه در عوض، قوانین و اعمال می‌توانند نوعی از دخالت

---

1. 11. See OMB Memo 04-04 to Federal Agencies
http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
2. But cf. Lawrence v. Texas,-U.S.-123 S. Ct. 2472, 2003 (recognizing that certain intrusions into individual privacy are beyond governmental power).

در رژیم خصوصی، به‌عنوان مثال تحقیقی در مورد اطلاعات زیست‌سنجی الکترونیک درخصوص یک فرد را جایگزین نوع دیگری از دخالت در حریم خصوصی نمایند (بازرسی بدنی پیش از ورود به یک تأسیسات). اما این بدین معناست که تحلیل‌گر نمی‌تواند قضاوت‌های ارزشی وسیعی نماید. هر شخصی سودمندی حریم خصوصی خویش را با معیار متفاوتی می‌سنجد. افراد معقول ممکن است درخصوص مواقع استفاده از فناوری زیست‌سنجی با یکدیگر اختلاف داشته باشند؛ اما اتخاذ این موضع که هرگونه استفاده‌ای از فناوری زیست‌سنجی دخالت در زندگی خصوصی است، مثل گفتن این است که سیستم‌های زیست‌سنجی در هر تعاملی باید مورد استفاده قرار گیرند. چالش خط‌مشی واقعی عبارت است از: یافتن کارآمدترین موارد استفاده از فناوری زیست‌سنجی معین (چه برای آزادی و چه برای امنیت) و نه برچسب کلی خیر یا شر زدن به آن.

بنابراین در تعیین درست اینکه چگونه می‌توان آزادی و امنیت را به بهترین وجهی در کنار هم تقویت نمود، سودمند خواهد بود که اصولی اساسی برای ارزیابی یک فناوری زیست‌سنجی داشته باشیم. چنین ضوابط اصولی باید شامل موارد زیر باشد:

- ثبت‌نام در سیستم‌های زیست‌سنجی باید آشکارا و نه مخفیانه باشد. پیش‌ازآنکه فردی در یک برنامه زیست‌سنجی ثبت‌نام شود، باید او را از این ثبت‌نام آگاه نمود. بنابراین ما به برنامه‌های زیست‌سنجی ازقبیل: تشخیص صورت عمومی که تصرف مخفیانه اطلاعات زیست‌سنجی را ممکن می‌سازند بدبین هستیم.
- سیستم‌های زیست‌سنجی در احراز هویت بهتر از تعیین هویت کارایی دارند؛ یعنی آنها تناسب بهتری برای تطابق نفر به نفر دارند که اطمینان می‌دهد یک شخص، همانی است که ادعا می‌کند و اجازه لازم برای شرکت در فعالیت موردنظر را داراست. فناوری‌های زیست‌سنجی به هنگام استفاده از روش انطباق فرد به جمع برای نفوذ در ناشناختگی فرد (به‌عنوان مثال درخواست دسترسی به مکانی خاص) به‌لحاظ خط‌مشی هم کارایی عملی کمتر و هم مسئله‌سازی بیشتری دارند.

● سیستم‌های زیست‌سنجی باید بیشتر برای کار کردن با ذخیره موضعی اطلاعات (مثلاً در الگوهای کارتی) طراحی شوند تا کار کردن با ذخیره مرکزی آنها. ذخیره تمرکزیافته اطلاعات زیست‌سنجی نگرانی‌هایی را در مورد حریم خصوصی برمی‌انگیزد و همچنین به اینکه به مأموریت‌های نفوذی آماده امکان بیشتری دهد، گرایش دارد.[1] واضح است که ذخیره موضعی اطلاعات برای برخی فناوری‌ها و کاربردها معقول نخواهد بود؛ اما تاآنجاکه درعمل امکان دارد باید ترجیح داده شود.

● ما به‌نحوی مشابه باید آن سیستم‌های زیست‌سنجی را بیشتر ترجیح دهیم که «اختیاری» و نیازمند رضایت شخصی هستند، تا آنهایی که اجباری‌اند. البته در اینجا منظور این نیست که نیاز به عمل اختیاری یک شخص نمی‌تواند شرط مشارکت لحاظ شود (به‌عنوان مثال اگر شما می‌خواهید وارد آمریکا شوید، باید یک سری اطلاعات زیست‌سنجی فراهم کنید)؛ زیرا مشارکت در نهایت داوطلبانه است. همچنین تصدیق می‌کنیم که کاربردهای خاصی از زیست‌سنجی (مثل: DNA برای تروریست‌های متهم‌شده) ممکن است نیاز به اجباری بودن داشته باشند. بااین‌حال این امر باید استثنایی بر قانون کلی داوطلبانه بودن باشد.

● به‌لحاظ دلایل مربوط به حریم خصوصی و امنیتی، فرد باید آن سیستم‌های زیست‌سنجی را که شاخص‌های زیست‌سنجی را به یک الگو کاهش می‌دهند بیشتر ترجیح دهد، تا آنهایی را که یک تصویر ذخیره‌شده را نگهداری می‌کنند. جعل الگوها در نوع خود، مشکل‌تر است. باوجوداین تصویرها ممکن است به نوعی راحت‌تر رمزگذاری شوند. در پایان، انتخاب این امر بستگی زیادی به مورد کاربرد دارد.

● درهرجا که امکان‌پذیر باشد، سیستم‌های زیست‌سنجی باید استفاده از اشکال ثابت‌شده

---

۱. در نتیجه ما همچنین از نیاز به صدور اجازه قانونی برای بسیاری از موارد استفاده فناوری زیست‌سنجی حمایت می‌کنیم. این شرط کافی به‌عنوان حفاظی در برابر مأموریت‌های نفوذی عمل می‌کند.

نام مستعار را در نظر بگیرند.

- هر نوع سیستم زیست‌سنجی باید برای جلوگیری از سوءاستفاده دارای برنامه‌های حسابرسی و نظارتی باشد. البته در مقاصد مربوط به امنیت ملی و اجرای قانون استثنائاتی نیز وجود دارد. توسل به این استثنائات باید کاملاً مستند و درمعرض بررسی ادواری باشد.
- هر سیستم زیست‌سنجی تنها به اندازه سیستم ثبت‌نامی ابتدایی قدرت دارد. یک راه ایده‌آل برای فرار از تشخیص سیستم زیست‌سنجی ثبت‌نام نامناسب در قالب استفاده‌کننده‌ای قانونی است. بنابراین همراه با به‌کارگیری هر سیستم زیست‌سنجی جدید باید به نظارت، حسابرسی و تست ادواری فرایند ثبت‌نام توجه داشت. اطلاعات ثبت‌نام همچنین باید درمعرض بازبینی ثانویه معمول جهت تشخیص مواردی که در مورد اول اشتباه ثبت‌نام شده‌اند باشد.
- یک سیستم زیست‌سنجی تنها به اندازه جایگزین کمک خویش قدرت دارد. اصل امنیت لایه‌بندی‌شده مستلزم این است که آن سیستم‌های درحال اجرای تعیین هویت زیست‌سنجی، یک سیستم تعیین هویت ثانویه مناسب را جهت استفاده در مواقعی که سیستم زیست‌سنجی اولیه خراب است یا نتیجه‌ای غیرقطعی حاصل می‌کند، در جای خویش محفوظ داشته باشند. اینکه یک سیستم کمکی زیست‌سنجی بخواهد برای مثال یک تأیید امضای غیرایمن ساده باشد، کفایت نخواهد کرد.

نکته پایانی اینکه فناوری‌های زیست‌سنجی می‌توانند درمورد حریم خصوصی افراد خنثی باشند. آنها می‌توانند و باید که با پروتکل‌های مناسبی طراحی شوند تا پیش از اجرا، حریم خصوصی افراد را تضمین کنند. این پروتکل‌ها هم می‌توانند جزئی از سخت‌افزار باشند (و لذا در داخل سیستم طراحی گردند) و هم ازطریق رهنمودهای عملیاتی و سیستم‌های نظارتی که به نگرانی‌های مربوط به حریم خصوصی می‌پردازند تقویت گردند.

فناوری پیشرفته، یک امتیاز رقابتی برای کشورها محسوب می‌شود و اگر قرار است

کشوری در جنگ علیه عوامل ضدامنیتی (مانند تروریسم) پیروز شود باید آن را مورد استفاده قرار دهد. در حقیقت مقاومت در برابر فناوری جدید خطرهای عملی را مطرح می‌سازد.

در هر حال به‌کارگیری فناوری‌های زیست‌سنجی جهت افزایش امنیت ملی سؤالات عملی و خط‌مشی متعددی را برمی‌انگیزد. این امر مسئله‌ای حیاتی است که نوع درست فناوری برای تحقق هدف و برآوردن اقتضاهای حریم خصوصی در یک مورد استفاده معین انتخاب گردد. به‌منظور اینکه سیستم‌های زیست‌سنجی امنیت ایجاد کنند، لازم است مردم برداشت غلطی از امنیت در مورد آنها نداشته باشند. ضعف‌ها و نقایص فناوری‌ها باید تصدیق شده، اقدامات پیشگیرانه مورد ملاحظه قرار گیرند. این سیستم‌ها نمی‌توانند به‌عنوان ابزار امنیتی غایی و لذا راه‌حلی کامل نگریسته شوند. به بیان دقیق‌تر، سیستم‌های زیست‌سنجی (در یک لایه یا بیشتر) صرفاً ابزاری دیگر در یک رویکرد لایه‌بندی‌شده به امنیت هستند. آنها دوای همه دردها نیستند؛ اما می‌توانند در حفاظت از یک کشور نقش مهمی بازی کنند و نباید به‌عنوان یک فناوری غیرقابل قبول، از آنها چهره‌ای شیطانی ساخت.

فصل هشتم
حفاظت از زیرساخت‌های حیاتی اطلاعاتی

- کالبد شکافی حفاظت از زیرساخت‌های حیاتی
- حفاظت از زیرساخت‌های حیاتی اطلاعاتی
- حفاظت از زیرساخت‌های حیاتی اطلاعاتی در کشورهای مدل

۱. کالبدشکافی حفاظت از زیرساخت‌های حیاتی[1]

۱ـ۱. مفهوم زیرساخت فضا و زیرفضا

زیرساخت‌ها به‌طورکلی مجموعه‌ای از عناصر ساختاری به‌هم پیوسته‌ای است که چارچوبی را برای پشتیبانی کردن از یک ساختار کلی ایجاد می‌کند. ازسوی‌دیگر زیرساخت‌ها شبکه‌ای از سرمایه‌های فیزیکی و سیستم‌هایی است که مبنا، کار پایه، موتور حرکت یا ظرف فعالیت‌های اقتصادی، سیاسی، نظامی، اجتماعی، فرهنگی، صنعتی، علمی و تکنولوژیکِ افراد، گروه‌های اجتماعی، نهادها، سازمان‌ها و دولت قرار می‌گیرد.

به‌بیان‌دیگر زیرساخت چارچوب اساسی یا ویژگی‌های یک سیستم یا سازمان و تأسیسات و تجهیزات مورد نیاز برای انجامِ درستِ کارهای یک کشور است. درمجموع با توجه به تعاریف ارائه‌شده، زیرساخت دارای شاخصه‌هایی همچون: یک سیستم بزرگ، با ابعاد تکنولوژیک گسترده، دارای ابعاد فیزیکی غیرقابل حرکت و ارائه دهنده خدمات پایه‌ای و اساسی است.

تعریف زیرساخت در شبکه، خود کمک مؤثری به درک و فهم آن می‌نماید. شبکه مجموعه‌ای از نقاط اتصال یا گره‌های به‌هم پیوسته و با ساختار باز است که می‌تواند بدون هیچ

---

۱. این متن اقتباسی است از:

علی عبداله‌خانی، «حفاظت از زیرساخت‌های حیاتی اطلاعاتی»، **مجله سیاست دفاعی**،سال چهاردهم، شماره ۵۴، بهار ۱۳۸۵، صص ۹۱ – ۱۲۸.

محدودیتی گسترش یافته و نقاط شاخص جدیدی را در درون خود پذیرا شود. البته تا زمانی‌که این نقاط توانایی ارتباط در شبکه را داشته باشند. با این تعریف شبکه‌های حمل‌ونقل، راه‌ها، آب، تلفن، سوخت، مالی، اطلاع‌رسانی، اینترنت، ارتباط رادیویی، اطلاعاتی و مواردی ازاین‌دست را می‌توان به‌عنوان زیرساخت معرفی نمود. برخی از این زیرساخت‌ها به‌صورت شبکه نبوده، بلکه به‌صورت مجموعه هستند؛ یعنی ویژگی‌های یک مجموعه را دارند؛ مانند مجموعه دانشمندان، دانشگاه‌ها و مراکز تحقیقاتی.

زیرساخت‌های شبکه‌ای دارای نقاط اتصال و خطوط هستند؛ به‌طور مثال در شبکه برق، نیروگاه‌ها، نقاط اتصال و کابل‌ها، خطوط انتقال محسوب می‌شوند. مجموعه‌ها نیز دارای اعضا هستند؛ مانند مجموعه دانشگاه‌ها که شامل دانشگاه تهران و دانشگاه صنعتی شریف و دیگر دانشگاه‌ها به عنوان عضو می‌شود.

هر زیرساخت دارای نقاط اتصال، گره یا عضو است که در مجموع خود را به‌صورت یک سازمان، نهاد یا تأسیسات نشان خواهد داد و خطوط و یا فضاهایی که خود را به‌صورت خطوط اتصال، خطوط انتقال، جریان‌های فرکانسی یا رادیویی و مواردی ازاین‌دست نشان می‌دهد.

در ذیل هر فضا یا گره و نقاط اتصال نیز زیرفضاها و زیرمجموعه‌ها وجود دارند که حلقه‌های اصلی و مرکز ثقل فضاها، گره‌ها و نقاط اتصال زیرساخت را تشکیل می‌دهند؛ به‌طور مثال شبکه مالی یک زیرساخت، بانک ملی مرکزی، یک نقطه اتصال یا گره، و مخزن نگهداری اسکناس و شمش‌های طلا یک زیرمجموعه یا حلقه به‌شمار می‌رود.

حلقه‌ها، زیرمجموعه‌ها یا زیرفضاها در هریک از فضاها یا نقاط اتصال متعلق به یک زیرساخت، به پنج دسته اصلی قابل تقسیم است. ما برای توضیح این مرحله از مفهوم زیرفضا ـ که بیشتر استفاده شده است ـ بهره می‌بریم.

اولین زیرفضا، **زیرفضای سرمایه‌ای** نام دارد که شامل کلیه سرمایه‌های منقولی است که در یک مکان نگهداری می‌شود. این سرمایه‌ها در چرخه کاری نهاد، سازمان، تأسیسات مربوطه به

عنوان فضا یا نقاط اتصال نقشی ندارند، بلکه خروجی (فراورده‌های تولیدی)، ورودی (مواد اولیه جهت مصرف که به‌طور موقت نگهداری می‌شوند) یا مواد آماده‌ای هستند که صرفاً برای مصرف برای مدتی نگهداری می‌شود؛ برای مثال شبکه حمل‌ونقل، یک زیرساخت است و بندر شهید رجایی یک نقطه اتصال یا گره در شبکه مذکور است. در این چارچوب محل‌های نگهداری، کانتینرهای حامل کالا یک زیرفضای سرمایه‌ای محسوب می‌شود. آن هم از زیرفضاهای نوع سوم، یعنی اینکه نه ماده اولیه است و نه خروجی و فراورده‌ی تولیدی، بلکه کالایی است که صرفاً به منظور انتقال برای مدتی در آنجا نگهداری می‌گردد.

دومین زیرفضا، **زیرفضای تأسیسات و تجهیزات** است. این زیرفضا در چرخه کار، ساختار و یا فرایند یک فضا یا نقطه اتصال و به‌طریق‌اولی در یک زیرساخت نقشی اساسی دارد؛ برای مثال زیرساخت شبکه آب کشور دارای مجموعه‌ای از ساخت‌هاست که سد کرج است یکی از آنها به‌شمار می‌رود. در این ساخت یا نقطه اتصال، توربین‌ها زیرفضای تأسیسات را تشکیل می‌دهند.

سومین زیرفضا، **ساختمان و سازه‌های یک ساخت** است. سازه‌ها و ساختمان درواقع فیزیک یک ساخت را تشکیل می‌دهد؛ به‌طور مثال شبکه تلفن کشور یک زیرساخت و برج مخابراتی تهران یکی از حلقه‌های اتصال این شبکه و ساخت بوده و سازه و ساختمان این برج یک زیرفضا یا حلقه‌ای از این ساخت محسوب می‌شود.

چهارمین زیرفضا، **عوامل انسانی** است. در برخی از ساخت‌ها، عوامل انسانی از اهمیت بسزایی برخوردار بوده، درواقع سرمایه اصلی را تشکیل می‌دهد. این عوامل در چرخه کار، ساختار یا فرایند یک ساخت اهمیت بالایی دارد؛ به‌طور مثال مجموعه دانشمندان کشور یک زیرساخت، سایت هسته‌ای نطنز یک ساخت یا حلقه اتصال، دانشمندان فعال در این سایت یک زیرفضا هستند.

پنجمین زیرفضا، **زیرفضای تبادل اطلاعات** است. زیرفضای تبادل اطلاعات شامل اطلاعات و ارتباطات و مواردی مانند: رایانه‌ها، نرم‌افزارها، اینترنت، ماهواره‌ها، بانک‌های

اطلاعاتی، آرشیو اسناد و مدارک می‌شود.

۱ـ۲. زیرساخت حیاتی و امنیت ملی

مفهوم زیرساخت حیاتی به‌طور طبیعی حکایت از نوعی تفکیک میان مجموعه‌ای از زیرساخت‌ها می‌کند که در یک تقسیم‌بندی کلی و حداقلی می‌توانند به دو نوع زیرساخت حیاتی و غیرحیاتی تقسیم شود. بدین‌ترتیب قائل به این هستیم که اهمیت برخی از زیرساخت‌ها نسبت به برخی دیگر بیشتر است. با توجه به این تفکیک به‌نظر می‌رسد زیرساخت‌های حیاتی را می‌توان به زیرساخت‌های مرتبط با امنیت ملی یک کشور مرتبط نمود. تقریباً تمامی امور، مسائل و پدیده‌های حیاتی درون یک کشور با امنیت ملی ارتباط دارند. این ارتباط نیز ناشی از گوهر امنیت است که ما را به مسئله وجود یا عدم وجود مدلول‌های خود و هرآنچه وجود آنها را تهدید نماید، ارجاع می‌دهد.

بنابراین می‌توان بر اساس تقسیم سطوح امنیت به امنیت فردی، اجتماعی[1]، دولت و کشور، به مصادیق زیرساخت‌های حیاتی نزدیک شد. در این چارچوب چنانچه حادثه امنیتی در زیرساختی موجب بروز ترس، دلهره یا وحشت در تک‌تک افراد یک جامعه از به‌خطر افتادن جان و مال آنان گردد، می‌توان آن را زیرساخت حیاتی نامید.

ازسوی‌دیگر چنانچه جان جمع کثیری از افراد که در زمان و مکانی مشخص و به‌صورت نوبه‌ای و مستمر اجتماع یا جمعیتی را تشکیل می‌دهند، بر اثر حادثه امنیتی در یک زیرساخت به خطر افتد یا حیات و چرخه فعالیت مجموعه‌ای از گروه‌های اجتماعی و یا سازمان‌های (به‌معنای تخصصی کلمه) حرفه‌ای، صنفی و شغلی بر اثر حمله یا آسیب‌پذیری و در نتیجه حادثه امنیتی در زیرساخت دچار توقف و یا آسیب جدی گردد، چنین زیرساختی را نیز می‌توان حیاتی تلقی نمود.

---

1. Social Security

مورد سوم به سطح امنیت دولت برمی‌گردد. در این چارچوب چنانچه حادثه امنیتی در زیرساختی منجربه تهدید علیه حیات یا چرخه فعالیت نهادهای اساسی دولت، فیزیک دولت و جریان ارتباطی دولت با بدنه خود و آحاد ملت گردد، چنین زیرساختی حیاتی قلمداد می‌گردد. همچنین چنانچه زیرساختی خودش سرمایه استراتژیک محسوب گردد یا آسیب دیدن کلی آن منجربه مخاطره سرمایه‌های استراتژیک دولت شود، سرمایه‌هایی که ارتباط وثیقی با تعهدات و تکالیف دولت نسبت به مردم کشور داشته یا برای حیات خود دولت ضروری است، چنین زیرساختی نیز حیاتی تلقی می‌گردد.

در آخر برخی از زیرساخت‌ها، مرتبط با بقاء یک کشور هستند؛ به‌گونه‌ای‌که حادثه امنیتی بر اثر حمله یا آسیب‌پذیری چنین زیرساختی تمام سطوح امنیت یک کشور را درهم‌نوردیده و با تهدید مواجه نماید. چنین زیرساخت‌هایی نیز حیاتی تلقی می‌گردند.

توضیحات ارائه‌شده تا حدودی می‌تواند مرز میان زیرساخت‌های حیاتی و غیرحیاتی را روشن کند؛ اما از این تقسیم‌بندی نمی‌توان نتیجه گرفت که هر زیرساخت حیاتی، مربوط به سطح به‌خصوصی از امنیت است، بلکه باید گفت آسیب‌دیدگی یا ازکار افتادگی زیرساخت‌های حیاتی به‌طورکلی بر چند سطح از سطوح امنیت تأثیر خواهد گذاشت و کمتر زیرساختی است که تبعات آسیب‌دیدگی آن صرفاً متوجه یکی از سطوح امنیتی شود.

۱ـ۳. تعاریف زیرساخت حیاتی

در اولین گام باید مشخص شود که به چه چیزهایی زیرساخت‌های حیاتی[1] اطلاق می‌شود. در پاسخ به این سؤال ابتدا می‌توان تعاریفی که تاکنون از این مفهوم ارائه شده را مورد بررسی قرار داد.

واژه‌نامه امریکن هریتیج[2] در تعریف زیرساخت به تسهیلات، خدمات و تأسیسات مورد نیاز جامعه‌ای کارآمد، ازجمله: سیستم‌های حمل‌ونقل و ارتباطات، آب، برق و مؤسسات

1. Cirital Infrastructure
2. The American Heritage Dictionary

عمومی نظیر مدارس، دفاتر پستی و زندان‌ها اشاره می‌کند.[1]

در حکم اجرایی حمایت از زیربناهای حیاتی در سال ۲۰۰۱ که توسط رئیس‌جمهور وقت آمریکا منتشر شده است، زیرساخت‌های حیاتی به تجهیزات، امکانات و خدمات تولید، تبدیل و توزیع برق، مخابرات و ارتباطات از راه دور؛ تجهیزات و امکانات تولید، استفاده، ذخیره و انهدام مواد و انرژی هسته‌ای؛ سیستم‌های اطلاعات دولتی و خصوصی؛ حمل‌ونقل اعم از: راه‌آهن، بزرگراه‌ها، بنادر و راه‌های آبی، فرودگاه‌ها و هواپیماها؛ دام، کشاورزی و سیستم‌های تهیه آب و غذا برای استفاده و مصرف انسان گفته شده است.[2]

در تعریف دیگری که در سند استراتژی ملی دولت بوش برای حمایت فیزیکی از زیربناهای حیاتی و دارایی‌های کلیدی در سال ۲۰۰۳ منتشر شده، دارایی‌ها و منابع کلیدی به سه دسته تقسیم گردیده‌اند: در دسته‌ی اول، طیف متنوع و گسترده‌ای از بناها، نمادها و مظاهر ملی، نمایانگر میراث، سنن و ارزش‌های ملی و قدرت سیاسی آمده است؛ مانند: بناهای تاریخی، نمادهای فرهنگی و مراکز دولتی و تجاری. در دسته‌ی دوم، تسهیلات و ساختارهایی نمایانگر قدرت اقتصادی و پیشرفت‌های تکنولوژیک، ازجمله: مراکز تجاری، دفاتر و ساختمان‌های اداری و استادیوم‌های ورزشی آورده شده است. در بخش سوم، تمامی مکان‌های عمومی که گردآورنده بخش اعظمی از مردم جهت اجرای فعالیت‌های تجاری، بازرگانی و شغلی، خرید یا تفریح هستند، آمده است.[3]

دولت انگلیس در گزارشی که تحت عنوان «محافظت از زیرساخت‌های حیاتی در کشور بریتانیا» منتشر کرده است،[4] زیرساخت‌های ملی حیاتی کشور را قسمتی از زیربناهای آن می‌داند که تداوم صحیح و مداوم آنها برای کشور حیاتی و از کار افتادگی، تأخیر طولانی در

---

1. John Moteff and Paul Parfomark, "Critical Infrastructure and Key Assests: Definition and Identification", **Science and Industry Division**, 2004, p. 2.
2. Ibid., p. 6.
3. "The National Strategy for Homeland Security", **U.S. Office of Homeland Security**, July 16, 2002, p. 30.
4. http://www.mio.gov.uk/output/page134.html

خدمات‌رسانی، قطع خدمات یا خدمات‌رسانی ناصحیح آنها موجب لطمات جدی به بدنه اقتصادی و اجتماعی گردیده، پیامدهای سنگینی برای دولت و جامعه در پی داشته، باعث بروز تهدیدات بالقوه و بالفعل برای کشور می‌شود. دولت انگلستان براساس این تعریف بخش‌های حیاتی خود را به ده قسمت اصلی و ۳۹ قسمت فرعی تقسیم می‌نماید که عبارتند از:

- ارتباطات (دیتا، مخابرات و تلفن، پست، اطلاعات ملی و بی‌سیم)؛
- خدمات اورژانسی (آمبولانس، آتش‌نشانی، پلیس و خدمات دریایی)؛
- منابع انرژی (الکتریسیته، گاز طبیعی و نفت)؛
- مالیات (مدیریت دارایی، امکانات مالی، سرمایه‌گذاری بانکی، بازار و بانکداری جزیی)؛
- غذا (تولید، واردات، فرایند، توزیع و خرده‌فروشی)؛
- دولت و خدمات عمومی و ملی (دولت مرکزی، دولت ایالتی، دولت محلی، پارلمان‌ها و مجلس‌های قانونگذاری، دادگستری و امنیت ملی)؛
- خطر و ایمنی ملی (تروریسم شیمیایی، بیولوژیکی، رادیولوژی و اتمی (CBRN) [1]؛ حوادث اجتماعی؛
- بهداشت (مراقبت بهداشتی و بهداشت عمومی)؛
- حمل‌ونقل (هوایی، دریایی، راه‌آهن و جاده)؛
- آب (آب مرکزی و فاضلاب)

در کشور استرالیا زیرساخت‌های حیاتی، بخش‌های بحرانی کشور معرفی شده است و گفته می‌شود که بخش‌های بحرانی، بخش‌هایی هستند که آسیب‌دیدگی آنها تأثیر بسیار شدیدی بر مسائل اجتماعی، اقتصادی و امنیت ملی دارد. برهمین‌اساس بخش‌های بحرانی و به‌طریق‌اولی زیرساخت‌های حیاتی در این کشور در قالب موارد ذیل تعریف شده‌اند:[2]

---

1. Chimical, Biological, Radiological, Nuclear Terrorism
2. M. Dunu and I. Wigert, "International CIIP Handbook", **Federal Institute of Technology Zurich, 2004.**

- ارتباطات (تلفن، فاکس، اینترنت، کابل و ماهواره‌ها و ارتباطات الکترونیکی)؛
- انرژی (گاز، سوخت نفتی، پالایشگاه، لوله‌کشی، تولید الکتریسیته و انتقال آن و راکتورهای هسته‌ای)؛
- سرمایه (بانکداری، بیمه و تبادلات تجاری)؛
- غذا (تولید انبوه، ذخیره‌سازی و پخش)؛
- بخش‌های دولتی (سیستم‌های جاسوسی و دفاعی، ساختمان‌های مجلس، بخش‌های کلیدی دولت، محل‌های اقامت مقامات، خدمات اورژانس مانند: آمبولانس و آتش‌نشانی)؛
- سلامتی (بیمارستان‌ها، سلامت عمومی، تحقیق و توسعه لابراتوارها)؛
- صنایع (صنایع سنگین و شیمیایی)؛
- موارد ملی (ساختمان‌های فرهنگی، ورزشی و گردشگری)؛
- ترابری (کنترل ترافیک هوایی، زمینی، دریایی و راه‌آهن)؛
- صنایع دفاعی (صنایع دفاع و شیمیایی).

در جمع‌بندی تعریف و تشریح زیرساخت‌های حیاتی می‌توان گفت که زیرساخت‌های حیاتی مجموعه عناصر ساختاری به‌هم پیوسته‌ای هستند که سیستم بزرگی را تشکیل داده، دارای ابعاد تکنولوژیک گسترده بوده، از ابعاد فیزیکی غیرقابل حرکت برخوردارند و خدمات اساسی و چارچوبی را برای پشتیبانی از ساختارهای کلان امنیت ملی کشور در سطوح امنیت کشور، امنیت دولت، امنیت جامعه و امنیت افراد و آحاد ملت است.

۱ـ۴. زیرساخت‌های حیاتی اطلاعاتی

همان‌طورکه در تعاریف روشن گردید، زیرساخت‌های حیاتی به دسته‌های مختلف تقسیم می‌شود؛ یکی از این مجموعه‌ها زیرساخت‌های حیاتی اطلاعاتی (CII) [1] هستند که برپایه و

---

1. Critical Information Infrastructure

بنیان فضای تبادل اطلاعات قرار دارند و درواقع زیرساخت‌های مربوط به *«فضای تبادل اطلاعات (فتا)»* به‌شمار می‌روند.

منظور از *«فضای تبادل اطلاعات»* مجموعه عوامل درگیر در تولید، ثبت، بازیابی، پردازش و انتقال اطلاعات شامل: تجهیزات پردازشی، تجهیزات راهگزینی و اتصال‌دهی شبکه‌ها، کانال‌های ارتباطی، نرم‌افزارهای سیستمی و کاربری و عوامل انسانی راهبر و کارگزار هستند.

زیرساخت‌های حیاتی اطلاعاتی مانند سایر زیرساخت‌های حیاتی به فضاها و زیرفضاها تقسیم‌بندی می‌شود. در این چارچوب زیرفضا شامل: تأسیسات و تجهیزات، پایگاه‌های داده‌ها، فضاهای انتقال، عوامل انسانی راهبر و کارگزار و برنامه‌هایی است که فضا، عملکرد خود را حول محور آن تنظیم می‌نماید.

برخی از فضاها و زیرفضاهای حیاتی اطلاعاتی مربوط به سایر زیرساخت‌ها است؛ یعنی زیرساخت‌های حیاتی غیراطلاعاتی، اما به جهت اهمیت زیرساخت در سطح حیاتی، فضا و زیرفضای اطلاعاتی آن مورد توجه قرار می‌گیرد.

آنچه از این پس مورد توجه قرار خواهد گرفت زیرساخت‌های حیاتی اطلاعاتی و فضاها و زیرفضاهای حیاتی اطلاعاتی مربوط به زیرساخت‌های حیاتی غیراطلاعاتی خواهد بود.

۲. حفاظت از زیرساخت‌های حیاتی اطلاعاتی

حفاظت[1] مترادف با ایمن‌سازی، و ایمن‌سازی مجموعه اقداماتی است که برای تبدیل شرایط موجود به شرایط امن یا مراقبت از تداوم شرایط امن صورت می‌گیرد.

حفاظت از زیرساخت‌ها و زیرفضاهای حیاتی اطلاعاتی مربوط به سایر زیرساخت‌های حیاتی موردنظر ماست که به دو بخش اصلی **حفاظت فیزیکی** و **حفاظت فضای رایانه** تقسیم می‌شود.

---

1. Protection

حفاظت فضای رایانه‌ها به‌معنای ایمن‌سازی **صحت**[1] و **محرمانگی**[2] منابع و داده‌های فضای رایانه‌ای است؛ درحالی‌که حفاظت فیزیکی بخشی از فرایند خارجی ایمن‌سازی فضای رایانه‌ای و مربوط به حفاظت بیرونی و خارجی از تجهیزات، سخت‌افزار، اماکن استقرار رایانه‌ها و شبکه‌های اطلاعاتی است.

برخی حفاظت فیزیکی از زیرساخت‌های اطلاعاتی و زیرفضاهای اطلاعاتی مربوط به سایر زیرساخت‌ها را در شمول حفاظت از امنیت فضای رایانه‌ای قرار نمی‌دهند؛[3] درحالی‌که برخی دیگر آن را بخشی از فرایند ایمن‌سازی فضای رایانه‌ای می‌دانند.[4]

پس از روشن شدن محدوده زیرساخت‌های موردنظر ـ که شامل زیرساخت‌ها و زیرفضاهای حیاتی اطلاعاتی مربوط به سایر زیرساخت‌ها می‌شود ـ به حفاظت فضای تبادل اطلاعات خواهیم پرداخت. بنابراین در اینجا حفاظت فیزیکی زیرساخت‌ها و زیرفضاهای حیاتی اطلاعاتی مطمح نظر ما نیست.

۲ـ۱. ارکان حفاظت

حفاظت از فضای رایانه‌ای همان‌طور که گفته شد، دارای دو رکن اساسی صحت و محرمانگی است. قبل از توضیح این دو مفهوم اساسی، باید به این سؤال پاسخ داد که صحت و محرمانگی چه عواملی در فضای رایانه‌ای باید حفاظت یا ایمن شود؟ پاسخ این است: عامل منابع و داده‌ها. منابع، کلیه اجزای فضای رایانه‌ای را شامل می‌شود که در شبکه دارای نقش و وظیفه به‌خصوصی هستند. و داده‌ها اجزایی هستند که در سیستم مورد پردازش قرار می‌گیرند. برای منابع مواردی مانند: دیسکت سخت، دستگاه کارت‌خوان، پردازنده‌های سیستم عامل، نرم‌افزار

---

1. Integrity
2. Confidentiality
3. Dorothy E. Denning, Peter J. Denning, "Data Security", **ACM Computing Surveys (CSUR)**, Vol. 11, No. 3, Sep. 1979, pp. 227-249.
4. Debra S. Herman, "A Practical Guide to Security Engineering and Information Assurance", **CRC Press**, 2008.

سرویس‌دهنده شبکه می‌توان نام برد و برای داده‌ها محتوای فایل‌های اطلاعاتی و پایگاه‌های اطلاعاتی را می‌توان مثال زد.[1]

با روشن شدن مرجع صحت و سلامتی که منابع و داده‌ها هستند، می‌توان حفاظت از فضای رایانه‌ای را به حفاظت از صحت و محرمانگی منابع، داده‌ها و اطلاعات ارجاع داد.

منظور از صحت درواقع سلامتی است؛ یعنی سلامتی منابع و داده‌ها و در تعریفی دقیق‌تر در این خصوص باید گفت یک منبع هنگامی صحیح شمرده می‌شود که کارکرد آن دقیقاً مطابق با رفتار مورد انتظار باشد؛ براین‌اساس صحت یا سلامتی منابع از طریق جذب، تغییر و افزودن موارد زائد به آنها یا نقض یکپارچگی‌شان تهدید می‌شود.[2]

صحت داده‌ها[3] صرفاً ازطریق اطمینان‌پذیری از منشأ اطلاعات مورد ارزیابی قرار می‌گیرد. بنابراین چنانچه معلوم گردد داده‌های دریافتی دقیقاً همان داده‌هایی است که از منشأ ارسال شده، این اطلاعات مهم ارزیابی می‌شود. لذا در اینجا درستی محتوای داده‌ها مطرح نیست، بلکه انطباق آنچه ارسال شده با آنچه دریافت شده مدنظر است.[4]

رکن دوم حفاظت، محرمانگی است. محرمانگی در برابر افشا و آشکار شدن قرار دارد و بیشتر در خصوص داده‌ها مطرح است تا منابع. البته برخی از منابع مانند نصب فایروال جزو منابع پنهان است و باید محرمانه بماند.

سیستم‌های حفظ و محرمانگی به سه دسته‌ی پنهان‌کاری[5]، اختفا[6] و سیستم‌های حقیقی محرمانگی[7] تقسیم می‌شوند. در سیستم پنهان‌سازی وجود داده‌ها یا منابع از دید حریف مخفی نگه داشته می‌شود؛ مانند انتقال داده‌ها ازطریق نامرئی‌نویسی. در سیستم اختفا، داده یا منبع در

---

1. James P. Anderson, "Computer Security Technology Planning Study", (http://Seclab.cs.ucdavis.edu/projects/history/paper/)
2. Cynthia E. Irvinc, Timothy E. Levin, "Data Integrity Limitations in Hybrid Security Architecture".(http://cisr.nps.navy.mil/downloads/dataintegrityhybrid.pdf).
3. Data integrity
4. Ibid.
5. Concealment
6. Privacy
7. True Secrecy

پوشش‌های دیگر قرار می‌گیرد؛ مانند انتقال صدا، اما ازطریق تحریف صدا یا قرار دادن فایل پنهانی در درون سایر متن‌های عادی. در سیستم‌های حقیقی محرمانگی داده‌ها یا منابع در دسترس است؛ اما آن داده یا منبع به‌صورت رمز درآمده و دسترسی به آن منوط به شکستن رمز است.[1]

۲ـ۲. ایمن‌سازی

مهم‌ترین سؤال در این بخش آن است که **حد ایمن‌سازی** در کجا قرار دارد؟ به عبارت دیگر، حفاظت و ایمن‌سازی فضای تبادل اطلاعات در چه مرحله‌ای باید صورت گیرد؟

ایمن‌سازی در سه وضعیت قابل برنامه‌ریزی است: وضعیت اول، *ظهور تهدید* است؛ یعنی با تمرکز بر تهدیدات صورت‌گرفته و مواردی مانند: شدت، عمق، جهت و هدف آن، برنامه‌ریزی جهت ایمن‌سازی یا حفاظت در این نقطه انجام خواهد شد. وضعیت دوم، **حمله** نام دارد؛ یعنی زمانی‌که تهدید به فعلیت درمی‌آید و مهاجم اقدام به حمله می‌نماید. وضعیت سوم، *حادثه امنیتی*[2] نامیده می‌شود. در این وضعیت، تهدید به فعلیت درآمده و بر اثر آن ظرفیت فضای تبادل اطلاعات صدمه دیده است. حادثه امنیتی، رویدادی است که نتیجه آن اختلال و آسیب دیدن سیستم است.

حادثه امنیتی از دو منبع ناشی می‌شود: اول، حمله توسط مهاجم و دیگری، ناشی از آسیب‌پذیری سیستم. حمله در چهار گام قابل تعریف است: استفاده از مجموعه‌ای از *ابزار* براساس استفاده از *آسیب‌پذیری‌های سیستم* و با *روش خاص*، به‌منظور *هدف قرار دادن یک یا مجموعه‌ای از عناصر سیستم*. چنانچه این اقدام به نتیجه منتج شود، حادثه‌ی امنیتی رخ داده است. در فضای تبادل اطلاعات حادثه امنیتی وقتی رخ می‌دهد که نفوذ به سیستم اتفاق افتاده باشد.

آسیب‌پذیری، نقص یا ضعف در طراحی، پیاده‌سازی و کارکرد یا مدیریت سیستم نامیده

---

1. C. E. Shamon, "Communication Theory of Secrecy Systems", **Bell System Technical**, Vol. 28, No. 4, pp. 656-715.
2. Security incident

می‌شود که در پاره‌ای موارد این آسیب‌پذیری مورد استفاده حمله‌کننده قرار می‌گیرد و گاهی نیز آسیب‌پذیری بدون فاعل منجربه حادثه امنیتی می‌شود.

با توجه به این سه وضعیت، دو رویکرد حفاظتی قابل تشخیص است. رویکرد اول *ایمن‌سازی* پیشینی نام دارد که برطبق آن پیش از وقوع هرگونه خطری باید تمام راه‌های محتمل بر روی آن بسته شود و از تمامی امکانات و ابزارها برای ایجاد مانع و سد به‌منظور عدم وقوع خطر استفاده گردد. این رویکرد منطبق بر وضعیت ظهور تهدید و حمله است؛ یعنی مبنا را بر دفع تهدید و منصرف کردن حریف از تهدید یا به بن‌بست کشاندن حمله قرار می‌دهد.

رویکرد دوم، *ایمن‌سازی* پسینی نام دارد. این رویکرد خطرها و تهدیدات را مادام که بالفعل نشده نادیده می‌گیرد و مبنای خود را وقوع حادثه امنیتی قرار می‌دهد؛ یعنی مشاهده شواهد یک حادثه امنیتی. وقتی چنین علائمی مشاهده شد، سیستم حفاظتی به‌طور واکنشی دست به کار شده، از صدمه دیدن امنیت فضای تبادل اطلاعاتی جلوگیری می‌کند. بنابراین مبنای این رویکرد، جلوگیری از به‌فعلیت درآمدن تهدید و حمله نیست، بلکه پس از آنکه حمله به وقوع پیوست، مبنای خود را به شکست کشاندن آن حمله قرار می‌دهد.

حال با توجه به وضعیت‌های سه‌گانه و رویکرد دوگانه ایمن‌سازی، به پاسخ سؤال اصلی این بخش یعنی حد ایمن‌سازی نزدیک می‌شویم. بدیهی است ایمن‌سازی باید معقول، مقرون‌به‌صرفه و منتج به موفقیت باشد. لذا ضرورتی ندارد که به ایمن‌سازی مطلق اندیشید؛ زیرا نباید هزینه‌های ایمن‌سازی از اصل آنچه باید حفاظت شود، بیشتر گردد. بنابراین هدف ایمن‌سازی را باید رسیدن به شرایط «اطمینان»[1] تعریف کرد.

در شرایط اطمینان اگرچه احتمال دارد مهاجم در حمله خود موفق گردد یا مدافع در شکست دادن حمله ناکام بماند، براساس شرایط موجود و به‌دلیل وجود میزانی از اطمینان، اقدامات انجام‌شده کافی تلقی می‌شود.

---

1. assurance

تعیین حد اطمینان و ایمن‌سازی براساس *میزان* ریسک محاسبه می‌شود و هرگاه میزان ریسک در حد قابل قبولی قرار داشته باشد، اقدامات انجام‌شده برای ایمن‌سازی حد مطلوب ارزیابی خواهد شد. در این چارچوب میزان ریسک را می‌توان به‌صورت حاصل‌ضرب احتمال موفقیت یک حمله در مقدار خسارت آن محاسبه نمود.[1]

روش‌های ایمن‌سازی: روش‌های ایمن‌سازی یا حفاظت، درخصوص صحت و محرمانگی داده‌ها و منابع مطرح می‌گردند. دراین‌میان برخی از روش‌ها بیشتر درخصوص صحت منابع و برخی دیگر درخصوص محرمانگی داده‌ها کاربرد دارند.

اولین روش که بیشترین کاربرد آن در محرمانگی داده‌ها و منابع است، *سیستم تشخیص نفوذ*[2] نام دارد که بیشتر به‌صورت یک طعمه عمل می‌کند. این سیستم اغلب آسیب‌پذیر و بی‌دفاع است و بیشتر برای فریب مهاجم و مشغول داشتن او به یک سیستم انحرافی طراحی می‌گردد.

روش دوم، بیشتر مرتبط با صحت داده‌هاست. این روش، *تصدیق هویت*[3] نام دارد. تصدیق هویت به معنای آن است که با استفاده از مکانیسم خاصی، از هویت یک موجود اطمینان حاصل می‌شود. تصدیق هویت روشی برای تشخیص صحت اطلاعات هویتی ارسال‌کننده اطلاعات است.

روش سوم، *کنترل دسترسی*[4] نام دارد. از این روش هنگامی استفاده می‌شود که مدیریت کل فضای تبادل اطلاعات در اختیار ما باشد.

این روش به‌عنوان یک سازوکار مراقبت از دسترسی‌های مستقیم و جلوگیری از دسترسی‌های غیرمجاز به فتا را برعهده دارد. در این سازوکارها، یک مرجع کنترلی، با واسطه شدن و مراقبت از تمامی دسترسی‌های صورت‌گرفته در یک حوزه، براساس مقررات

---

1. Bob Blakley, Ellen McDemott, Dan Geer, "Information Security is Information risk management", **Workshop on New Security Paradigms**, Sept. 2001, pp. 97-104.
2. Intrusion Detection System 3. authentication
4. access control

تعیین‌شده، دسترسی‌ها را پیش از انجام ارزیابی می‌کند و تنها بـه دسترسـی‌هـای مجـاز امکـان ورود می‌دهد.

روش چهارم، *نهان‌نگاری*[1] نام دارد. این روش بیشتر برای محرمانگی داده‌ها مـورد اسـتفاده قرار گرفته، تلاش دارد تا با پنهان کردن داده‌های محرمانـه در دل تـوده‌ای از داده‌هـای عـادی، محرمانگی داده‌های محرمانه را حفظ کند.

روش پنجم، *رمزنگاری*[2] است. در این روش، ظاهر نمایش داده‌ها به شکل خاصی است که فقط برای افرادی که کلیـد آن را در اختیـار دارنـد قابـل خوانـدن اسـت. ایـن روش یکـی از مرسوم‌ترین و مناسب‌ترین روش‌های حفظ محرمانگی داده‌ها محسوب می‌شود.

روش ششم، *کنترل جریان اطلاعات*[3] نام دارد و بـه‌دنبـال کنتـرل نقـل مکـان اطلاعـات در فناست. در حقیقت این روش می‌خواهـد مـستقل از کنتـرل دسترسـی‌هـا، از تغییراتـی کـه در اطلاعات منتقل‌شده ایجاد می‌شود، جلوگیری نماید. بنابراین در این روش دسترسی بـه ظـرف نگهداری اطلاعات[4] کنترل می‌گردد.

۲ـ۳. سیاست‌های امنیتی

سیاست امنیتی دقیقاً براساس حد ایمن‌سازی ضروری و لازم می‌آیـد. در ایمـن‌سـازی و بـرآورد ریسک، صرفاً از متغیرهای کمی استفاده نخواهد شد و بسیاری از متغیرهای کیفی و عناصر نـسبی و اعتباری در این زمینه مؤثر و مطرح هستند. درواقع با تعیین مجموع پارامترها و متغیرهاست کـه می‌توان سطح قابل اطمینان تأمین امنیت و ایمن‌سازی را در یک حوزه معین مشخص کـرد. مـثلاً اینکه چه دارایی‌هایی باارزش هستند و امنیت آنها مهم است، کدام دارایی‌ها محرمانه هستند و چه کسانی تا چه حد می‌توانند به آن دسترسی داشته باشند، هزینه ریـسک قابـل تحمـل چـه مقـدار

---

1. Steganography
2. Cryptography
3. Information flew Control
4. Information Container

است. اینها نمونه‌هایی از عناصر قراردادی و اعتباری است که تعیین وضعیت نسبت به هر یک از آنها در قالب مجموعه‌ای تحت عنوان سیاست‌های امنیتی گنجانده می‌شود.

سیاست‌های امنیتی مشخص می‌کند که پارامترهای متغیر و نسبی موجود در ایمن‌سازی، در حوزه‌ای خاص چگونه هستند و در یک کلام، سیاست امنیتی میان انتظارات و ضوابط امنیتی در حوزه‌ای خاص چگونه است؛ به‌طور مثال در حوزه زیرساخت‌ها و زیرفضاهای مربوط به تبادل اطلاعات، سیاست امنیتی فایروال به‌معنای قواعدی است که تعیین می‌کند کدام بسته‌ها باید از فایروال عبور داده شوند و کدام‌یک مجاز به عبور نیستند.[1] این نوع سیاست‌ها در مجموعه سیاست‌های کنترل دسترسی قرار می‌گیرند.

هدف از تدوین سیاست‌های امنیتی که درواقع تعیین‌کننده حدود و معیارهای حفاظت هستند آن است که کاربران، کارمندان و مدیران نسبت به حدود و معیارها و ضوابط مربوط به کارها و فعالیت‌های ایمن‌سازی دارایی‌های اطلاعاتی آشنا گردند و بدانند انجام فعالیت‌ها، برنامه‌ها و اهداف باید در چه چارچوبی دنبال شود.

سیاست‌های امنیتی در زیرساخت‌ها و زیرفضاهای حیاتی تبادل اطلاعاتی را در سه سطح می‌توان دسته‌بندی نمود: سیاست‌های امنیتی برنامه‌ریزی، سیاست‌های موضوعات خاص و سیاست‌های سیستمی.

سیاست‌های سطح برنامه‌ریزی برای ایجاد یا بازسازی برنامه‌های ایمن‌سازی تدوین می‌شوند. سیاست‌های سطح موضوعات خاص آن دسته از سیاست‌هایی هستند که تنها در حوزه‌ای خاص که در مقطع زمانی موردنظر مورد توجه قرار گرفته تمرکز می‌یابند. چنین تمرکزی از ظهور فناوری‌های جدید در سیاست‌های جدید دولت و بروز حوادث جدید در حوزه‌ای خاص ناشی می‌شود، و در آخر، سیاست‌های سطح سیستمی سیاست‌هایی هستند که تنها در حوزه یک سیستم خاص از کل سازمان کاربرد دارند.

---

1. K. Honc, J. H. P. Eloff, "Information Security Policy: What do International Security Standard Say?", **Computer and Security**, Vol. 21, No. 5, pp. 402-409.

۳. حفاظت از زیرساخت‌های حیاتی اطلاعاتی در کشورهای مدل

۳ـ۱. آمریکا

ساختار و سازمان: آمریکا در زمینه فناوری اطلاعات و ارتباطات و به‌ویژه امنیت اطلاعات و ارتباطات، یکی از کشورهای پیشرو محسوب می‌شود که ساختارها، سازمان‌ها و فرایندهای گسترده و پیچیده‌ای دراین‌خصوص دارد و پس از حادثه یازده سپتامبر ۲۰۰۱ نیز آنها را مورد بازنگری جدی و اساسی قرار داد؛ به‌طوری‌که تا قبل از این سازمان‌ها و نهادهای متعدد و تقریباً مستقلی در این زمینه‌ها فعالیت می‌کردند؛ اما درحال‌حاضر بخش عمده‌ای از ساختارها، سازمان‌ها و فرایندهای مربوطه در داخل تشکیلات جدیدی تحت عنوان «وزارت اطلاعات امنیت داخلی (DHS)[۱]» سازماندهی گردیده است.

وزارت امنیت داخلی از پنج بخش اصلی شامل: *مدیریت*، *علوم و تکنولوژی*، *پاسخگویی و آماده‌سازی در موارد اضطراری*؛ *امنیت مرزها و ترابری*، و *تحلیل اطلاعات و محافظت از زیرساخت‌ها* تشکیل شده که بخش مرتبط با فضای تبادل اطلاعات و درواقع مهم‌ترین بخش مرتبط با موضوع مقاله، یعنی بخش *تحلیل اطلاعات و محافظت* از زیرساخت‌ها (IAIP)[۲] است و این بخش از دو اداره *تحلیل اطلاعات (IA) و اداره محافظت از زیرساخت‌های حیاتی (IP)* تشکیل گردیده است. در چارچوب IAIP دو برنامه عمده سازماندهی گردیده شده‌اند که برنامه *امنیت اطلاعات*[۳] و *حفاظت از زیرساخت‌های اطلاعاتی حیاتی*[۴] نام دارند.[۵]

---

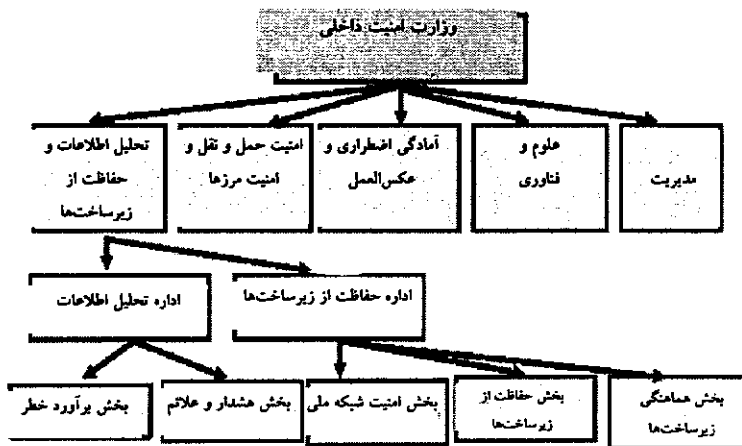
1. Department of Homeland Security

۲. IAIP (Information Analysis and Infrastructure Protection) یکی از پنج بخش دپارتمان امنیت کشور آمریکاست. مسئولیت این بخش شناسایی و ارزیابی تهدیدات جاری و آینده و نیز آسیب‌پذیری‌های کشور، هشدارهای به‌موقع و عملکردهای جلوگیری کننده و حفاظتی است. به‌طور خاص می‌توان گفت که بیشترین توجه این بخش بر حفاظت ساختارهای حیاتی و امنیت فضای سایبر است. علاوه بر این IAIP وظیفه هماهنگی فعالیت‌ها در جهت حفظ ساختارهای ملی و ایجاد ارتباط فعال با بخش خصوصی را نیز دارد. همچنین IAIP وظیفه تحلیل اطلاعات به‌دست‌آمده از منابع مختلفی را به عهده دارد که این منابع شامل FBI، CIA، آژانس جاسوسی دفاع و آژانس امنیت ملی می‌شوند.

3. Information Security (InfoSec)

4. Critical Information Infrastructure Protection (CIIP)

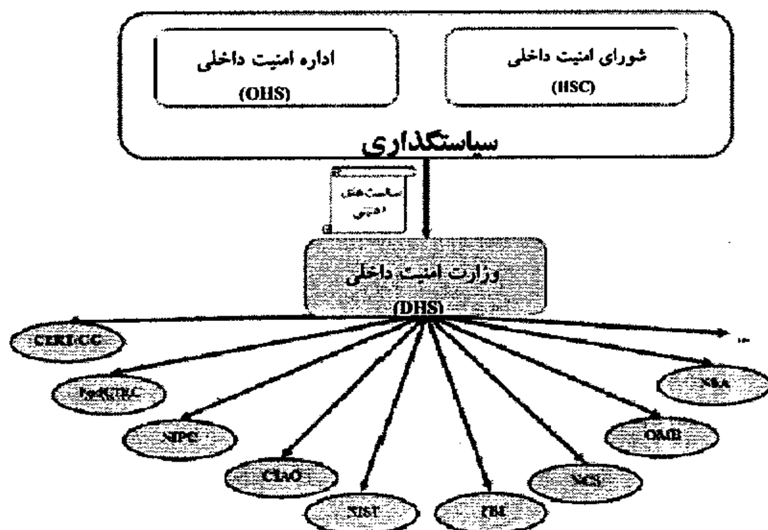
5. http://www.dhs.gov.dhspublic/theme_home1.jsp



شکل ۱. ساختار وزارت امنیت داخلی آمریکا

سیاستگذاری برنامه‌های مربوط به InfoSec در بخش IAIP توسط دو نهاد مستقل به نام، *اداره امنیت داخلی (OHS)* [1] و *شورای امنیت داخلی (HSC)* [2] انجام می‌شود. در این چارچوب OHS مسئولیت طراحی و هماهنگی کلیه فعالیت‌ها و سازمان‌های دولتی را با هدف اجرای استراتژی ملی محافظت از کشور آمریکا در مقابل تهدیدات و حملات تروریستی برعهده دارد. همچنین HSC مشاور رئیس‌جمهور در امر سیاستگذاری و هماهنگی سازمان‌ها و آژانس‌های دولتی در اجرای سیاست‌ها در کلیه زمینه‌های فعالیت وزارت امنیت داخلی است.[3]

1. Office of Homeland Security (OHS)
2. Homeland Security Council (HSC)
3. Ibid.



شکل ۲. سازماندهی برنامه امنیت اطلاعات آمریکا

علاوه بر سیاستگذاری مستقل مربوط به InfoSec سیاستگذاری مربوط بـه CIIP از بخـش IAIP نیز به‌صورت مستقل، اما برخلاف مورد قبلی به‌طـور متمرکـز انجـام مـی‌شـود؛ یعنـی از همکاری دیگر سازمان‌های دولتی برای سیاسـتگذاری اسـتفاده نمـی‌شـود. بـاوجوداین اجـرای برنامه‌ها توسط دستگاه‌های متولی زیرساخت‌های حیاتی، و تحلیل مدیریت و مخاطرات مربوط به این برنامه توسط IA [1] انجام خواهد گرفت.

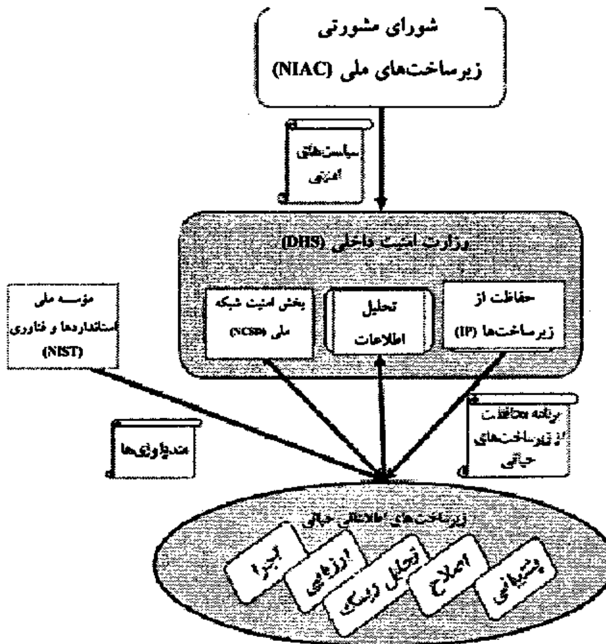
با توجه به متمرکز بودن سیاستگذاری، شورایی تحت عنوان «*شورای مـشورتی زیرسـاخت ملی*» (NIAC)[2] مسئولیت سیاستگذاری مربوط به CIIP را برعهده دارد. ایـن شـورا زیـر نظـر رئیس‌جمهور سیاستگذاری پیرامون زیرساخت‌هـای حیـاتی در عرصـه‌هـای مختلـف را انجـام می‌دهد. این شورا سی عضو دارد که توسط شخص رئیس‌جمهـور و از میـان خبرگـان بخـش خصوصی، دولت مرکزی، دولت‌های محلی، دانشگاه‌ها انتخاب می‌شوند.

---

1. Information Analysis
2. National Infrastructure Advisory Council (NIAC)

مسئولیت‌های این شورا عبارتند از:

- پیشنهاد و توسعه راه‌هایی برای تشویق بخش خصوصی به انجام ارزیابی خطرها به طور متناوب؛
- گسترش و نظارت بر مراکز تحلیل و تسهیم اطلاعات (ISAC) [1] در بخش‌های خصوصی[2]؛
- هماهنگ‌کننده ISACها.



شکل ۳. سازماندهی برنامه محافظت از زیرساخت‌های اطلاعاتی حیاتی آمریکا

1. Information Sharing and Analysis Center

۲. وظیفه‌ی ISACها جمع‌آوری و پخش اطلاعات، رویدادها و پاسخ‌دهی به آن از طریق اعضای آن و تسهیل تبادل اطلاعات مابین دولت و بخش خصوصی می‌باشد.

زیرساخت‌های حیاتی: آمریکا دارای بخش‌های مهم و حساسی است که مهم‌ترین آنها که در چارچوب زیرساخت‌های حیاتی این کشور گنجانده شده‌اند، عبارتند از:

کشاورزی، غذا، آب، سلامتی، خدمات اضطراری، بنیان‌های صنعتی دفاع، ارتباطات و اطلاعات، انرژی، ترابری، سرمایه‌گذاری و بانکداری، صنعت شیمیایی، پست، و حمل‌ونقل.[1]

طرح‌ها و استراتژی‌ها: حفاظت از زیرساخت‌های حیاتی اطلاعاتی (CIIP) که به‌عنوان یک برنامه در بخش IAIP توضیحات آن داده شد، در قالب طرحی استراتژیک تحت عنوان «*طرح ملی برای محافظت از سیستم‌های اطلاعاتی*[2] به مرحله اجرا درمی‌آید.[3]

این طرح دارای سه فصل و ده برنامه به شرح زیر است:

- **آماده‌سازی و پیشگیری:**

ـ **برنامه اول:** شناسایی دارایی‌های زیرساخت‌های حیاتی، وابستگی‌ها و تشخیص آسیب‌پذیری‌ها.

- **تشخیص و مقابله:**

ـ **برنامه دوم:** تشخیص حملات و نفوذهای غیرمجاز؛

ـ **برنامه سوم:** ایجاد و توسعه سیستم‌های اطلاعاتی و مجری قانون؛

ـ **برنامه چهارم:** به اشتراک‌گذاری سریع هشدارهای حملات؛

ـ **برنامه پنجم:** تهیه امکانات لازم جهت پاسخگویی، نوسازی و بازیافت؛

- **ایجاد شالوده قوی:**

ـ **برنامه ششم:** توسعه بخش تحقیقات و توسعه؛

ـ **برنامه هفتم:** آموزش و استخدام متخصصان امنیت ـ اطلاعاتی؛

1."National Strategy for homeland Security",Op.cit., p. 41.

2. National Plan for Information System Protection

3. "National Plan for Information Systems Protection, **The White House**, Version 10, 2003, pp 13-14

ـ **برنامه هشتم:** آگاهی‌رسانی به مردم آمریکا نسبت به نیاز به بهبود امنیت فضای تبادل اطلاعات؛

ـ **برنامه نهم:** وضع قوانین مقتضی برای پشتیبانی مناسب از برنامه؛

ـ **برنامه دهم:** در هر بند و مرحله از برنامه، نسبت به حفظ دارایی‌ها، داده‌ها، آزادی‌های مدنی و حقوق حریم خصوصی اطمینان حاصل شود.

علاوه‌بر طرح ملی برای محافظت از سیستم‌های اطلاعاتی، طرح ملی آمریکا درخصوص InfoSec در چارچوب وزارت امنیت داخلی BHS و ذیل بخش IAIP تحت عنوان *«راهبرد ملی برای امنیت فضای تبادل اطلاعات»*[1] تدوین و در سال ۲۰۰۳ به تصویب رئیس‌جمهور این کشور رسیده است.[2] این طرح دارای سه هدف شامل موارد ذیل است:

۱. جلوگیری از حمله علیه زیرساخت‌های حیاتی آمریکا؛

۲. کاهش آسیب‌پذیری‌های ملی در برابر حملات رایانه‌ای؛

۳. حداقل کردن خسارت و زمان بازیافت در برابر حملات رایانه‌ای.

علاوه‌بر اهداف فوق در راهبرد ملی به برنامه‌ریزی درخصوص پنج اولویت زیر تأکید فراوان شده است:

اولویت اول: سیستم ملی پاسخگویی به امنیت فضای تبادل اطلاعات؛

اولویت دوم: برنامه ملی کاهش تهدیدات و آسیب‌پذیری‌های فضای تبادل اطلاعات؛

اولویت سوم: برنامه ملی آگاهی‌رسانی و آموزش امنیت فضای تبادل اطلاعات؛

اولویت چهارم: ایمن‌سازی فضای اطلاعات دولت؛

اولویت پنجم: همکاری امنیت ملی و امنیت فضای تبادل اطلاعات بین‌المللی.

روش‌شناسی تحلیل مخاطرات در آمریکا: سیستم پاسخگویی و روش‌شناسی تحلیل

---

1. The National Strategy to Secure Cyber Space
2. "The National Strategy to Secure Cyber Space", **The White House**,2003, pp. 9-13.

مخاطرات در آمریکا دارای چهار حلقه: *تحلیل، هشدار، مدیریت رویداد، و پاسخگویی و بازسازی* است.[۱]



توانایی‌ها/ اجزا

برنامه‌های پاسخگویی ملی به حوادث
- برنامه‌های فدرال
- برنامه هماهنگی فردی

ساختار مدیریت رویداد DHS
- هماهنگی فدرال
- هماهنگی فردی، دولتی و محلی

مرکز عملیات‌های رویداد DHS
- شبکه اطلاعات و هشدار سایبر
- مراکز تحلیل و تسهیم اطلاعات (ISAC'S)

مرکز تحلیل DHS
- گروه استراتژیک
- گروه تاکتیکی
- برآوردهای آسیب‌پذیری

شکل ۴. سیستم پاسخگویی و تحلیل مخاطرات در آمریکا

روش استاندارد تحلیل مخاطرات مربوط به امنیت اطلاعات در سیستم‌های امنیتی آمریکا OCTAVE[۲] نام دارد.[۳] این روش به‌منظور ارزیابی خطرهای مربوط به امنیت اطلاعات و تحلیل مخاطرات مربوط به زیرساخت‌های حیاتی اطلاعات به‌کار گرفته می‌شود. روش مزبور دارای خط مشی سه مرحله‌ای است و هر مرحله نیز خود چندین زیرمجموعه دارد. این روش در چارچوب تکنیک‌های تحقیقاتی گروهی به‌ویژه دلفی انجام می‌شود.

مراحل سه‌گانه و اساسی این روش برای تحلیل مخاطرات به شرح زیر است:

- مرحله اول: مشخص کردن تمامی تهدیدات علیه سرمایه‌های حیاتی؛
- مرحله دوم: مشخص کردن آسیب‌پذیری‌های مربوط به سرمایه‌های حیاتی؛
- مرحله سوم: گسترش استراتژی امنیت و طرح‌ها، در این مرحله طرح‌ها، برنامه‌ها و

---

1. Ibid., p. 17.
2. Opertionally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
3. Mikhail Sonsonkin, "Operationally Critical threat, Asset and Vulnerability Evaluation", **Polytechic University**, 2005.

راهبردها برای مواجهه با مخاطرات اتخاذ می‌شود.

علاوه‌براین پنج اصل اساسی در استانداردهای تحلیل مخاطرات مربوط به امنیت اطلاعات در آمریکا و در چارچوب بخش IAIP مورد توجه قرار می‌گیرد.

	معیارهای ارزیابی	برنامه‌ها	آسیب‌پذیری‌ها	دارایی‌های حیاتی	تهدیدات
Private Sector	میزان تأثیر برنامه‌های شما چقدر است؟	چه برنامه‌هایی برای حفاظت از دارایی‌های حیاتی خود دارید؟	آسیب‌پذیری‌های مشترک و منفرد دارایی‌های شما چیست؟	دارایی‌های حیاتی شما چیست و محل آنها کجاست؟	چه تهدیداتی فراروی سازمان شماست؟ (تاکتیکی یا استراتژیک)
Government	دولت از چه معیارهایی برای ارزیابی موفقیت برنامه ملی استفاده می‌کند؟	دولت چگونه می‌تواند در پر کردن شکاف‌های موجود در فعالیت صنعت کمک کند؟ (برنامه یا فناوری؟)	وابستگی‌های بین صنعت و زنجیره عرضه (تأمین) چیست؟	چه شیوه‌ای را باید دولت برای حلقه‌بندی دارایی‌های حیاتی به‌کار گیرد؟	باید چه اطلاعاتی از سوی دولت به شما برای تهدیدات داده شود؟

شکل ۵. پنج اصل برای حفاظت از ساختارهای حیاتی

در آمریکا مدیریت تحلیل مخاطرات براساس تعیین بخش‌های بحرانی و به‌دنبال آن تعیین فضاهای حائز اهمیت تبادل اطلاعات در بخش‌های بحرانی شکل می‌گیرد. با توجه به این دو اقدام، بخش‌های تحلیل و بررسی مخاطرات در IA-IP تشکیل می‌شوند و در هریک از این دو بخش ـ که زیرمجموعه IAIP هستند ـ تحلیل مخاطرات مربوط به همان مجموعه صورت می‌گیرد. بااین‌حال تحلیل مخاطرات در دو سطح کلان و بخش‌های بحرانی انجام می‌شود. در سطح کلان سیاستگذاری‌ها و تحلیل مجموع مخاطرات در بخش‌های مختلف و تأثیرات آن بررسی می‌شود و در سطح بخش‌های بحرانی، تحلیل مخاطرات توسط ISACها انجام می‌شود.

۳ـ۲. استرالیا

ساختارها و سازمان‌ها: سه وزارتخانه دفاع، دادگستری و ارتباطات اصلی‌ترین نقش را درخصوص حفاظت از فضاهای حیاتی تبادل اطلاعات در استرالیا برعهده دارند. دراین‌میان نقش اجرایی وزارت دفاع و نقش سیاستگذاری وزارت ارتباطات مشهودتر و مؤثرتر است.[۱]

در ذیل وزارت دفاع مجموعه‌ای تحت عنوان «اداره سیگنال‌های دفاعی» (DSD)[۲] وظیفه حفاظت از شبکه‌های اطلاع‌رسانی، مواجهه با تهدیدات و مخاطرات رایانه‌ای را برعهده دارد و نیز مسئول هشدار دادن به سازمان‌ها و ادارات ایالتی درخصوص انجام عملیات امنیتی در حوزه IT است. DSD مأموریت‌های خود را در چارچوب دو بخش امنیت اطلاعات (InfoSec) و اطلاعات سیگنالی انجام می‌دهد. اطلاعات سیگنالی درواقع وظیفه شنودها و ضدشنودها را در سطح ملی برعهده دارد.

DSD همچنین سه برنامه مؤثر را برای انجام وظایف طراحی کرده است که شامل: *گزارش حوادث*[۳]، *تیم آسیب‌پذیری شبکه‌های رایانه‌ای (CNVT)*[۴] و *برنامه گواهی‌های مدخل*[۵] هستند.

برنامه گزارش حوادث به شفاف‌سازی وقایع موجود در حوزه امنیت و ارائه گزارش و تحلیل درباره آن می‌پردازد. گزارش‌های این مجموعه کارپایه تعیین تهدیدات و تولیدهای امنیتی می‌گردد. حوادثی که در این مجموعه درخصوص آن گزارش تهیه خواهد شد، مواردی مانند: ورود غیرمجاز به سیستم IT، وارد نمودن سهوی و عمدی ویروس‌ها به شبکه و تخریب و بهره‌برداری‌های غیرمجاز از اطلاعات حفاظت‌شده است.

تیم CNVT یکی از برنامه‌های مهم در ذیل سازمان DSD است. این تیم مرکب از عناصر بسیار حرفه‌ای استرالیا در زمینه IT است که هدف تشخیص بنیان‌های آسیب‌پذیری شبکه فتا دولتی را دنبال می‌کند.

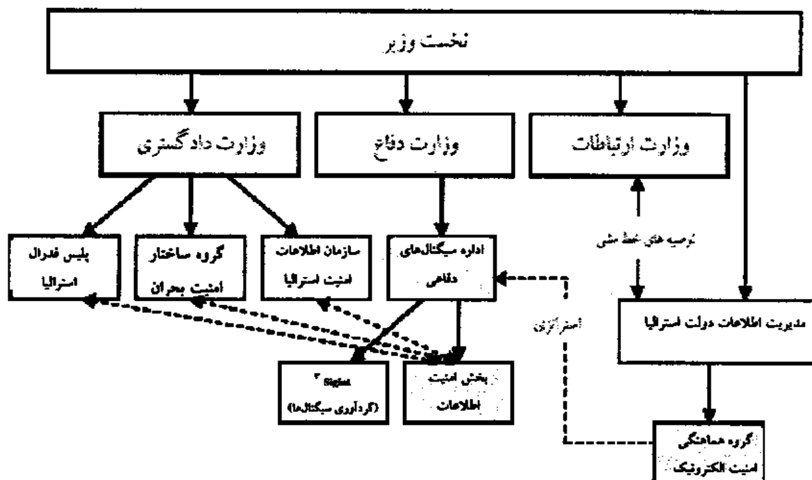
---

1. M. Dunn and I. Wigert, Op.cit., Part Australian.
2. Defence Signals Directorate
3. Ineident Riporting
4. The Computer Network VulnerohilityTeam
5. Gateway Certification

برنامه سوم که گواهی‌های مدخل نام دارد، برای کمک به آن دسته از سازمان‌های دولتی که به شبکه اینترنت وصل شده‌اند ایجاد شده است. هدف اصلی این مجموعه کاهش خسارت و مخاطرات ورود به شبکه اینترنت توسط کاربران مذکور می‌باشد.

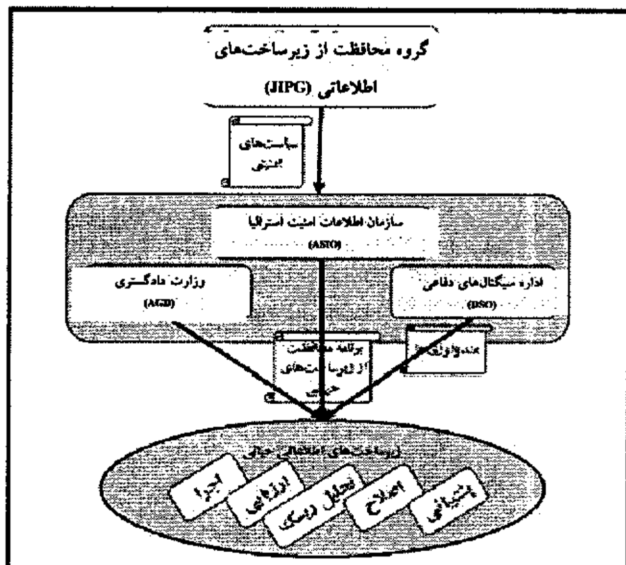
سازمان *مدیریت اطلاعات دولت استرالیا* (AGIMO) [1] یکی دیگر از تشکیلات درگیر در امنیت فضاهای حیاتی تبادل اطلاعات (افتا) است. این سازمان که زیرنظر وزارت ارتباطات است، وظیفه کلان تعیین خط‌مشی دولتی در کلیه زمینه‌های مرتبط با افتا را برعهده دارد. توسعه محیط الکترونیکی امن و قابل اعتماد، افزایش آگاهی در زمینه امنیت الکترونیکی، و تهیه گزارش از وقایع، از دیگر وظایف این سازمان به‌شمار می‌رود.

گروه ساختار امنیت بحران (CIPG) [2] که در ذیل وزارت دادگستری قرار دارد نیز یکی دیگر از سازمان‌های اصلی درگیر در زمینه افتاست. این سازمان وظیفه تشخیص مخاطرات و تعیین و ارزیابی آسیب‌پذیری در بخش‌های بحرانی مخابرات، مالی، الکتریسیته و کنترل ترافیک هوایی را برعهده دارد.



شکل ۶. ساختار امنیت اطلاعاتی در استرالیا

1. Australian Government Information Management (AUIMO)
2. Critical Infrastructure Protection Group (CIPG)
3. Signals Intelligence

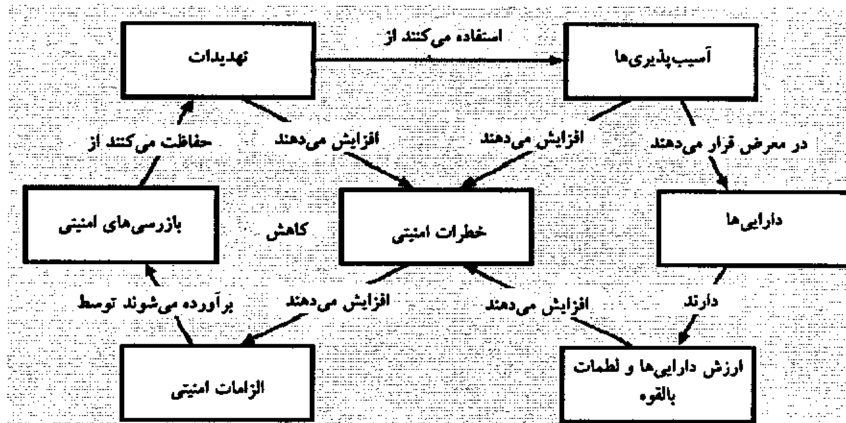


شکل ۷. سازماندهی برنامه‌ی حفاظت از زیرساخت‌های حیاتی در استرالیا

روش‌شناسی تحلیل مخاطرات: استرالیا دارای یک استاندارد مدیریت خطر است که در چارچوب آن همه ساختارهای بحرانی به‌منظور مدیریت خطر برای *جلوگیری، آمادگی و پاسخگویی و بازسازی* ارزیابی می‌شوند. نظام‌نامه امنیتی تکنولوژی اطلاعات دولت[1]، استانداردهای استرالیا برای تحلیل مخاطرات در حوزه افتا را شکل داده است.[2]

اجزای این نظام‌نامه شامل: *سرمایه‌ها، ارزش سرمایه‌ها، تهدیدات، آسیب‌پذیری‌ها، خطر امنیتی، نیازهای امنیتی و کنترل‌های امنیتی* است.

1. ACSI23 Government IT Security Manual
2. "Australian Government Information Technology Security Manual", **Defence Signals Directorate**, 2004, pp. 1-4.



شکل ۸ نمای کلی روابط در مواجهه با خطر در استرالیا

علاوه بر روش‌شناسی تحلیل مخاطرات که به عنوان صفحه استاندارد تحلیل مخاطرات عمل می‌نماید، در استرالیا مدیریت مواجهه با مخاطرات (ERM) [1] توسط سازمانی تحت عنوان مدیریت فوریت‌های استرالیا (EMA) [2] انجام می‌پذیرد. مدیریت مواجهه با مخاطرات در واقع فرایند بررسی، تحلیل و ارزیابی مخاطرات استرالیا در حوزه افتاست که براساس سند استاندارد روش‌شناسی تحلیل مخاطرات این فرایند تحقیق می‌یابد.[3]

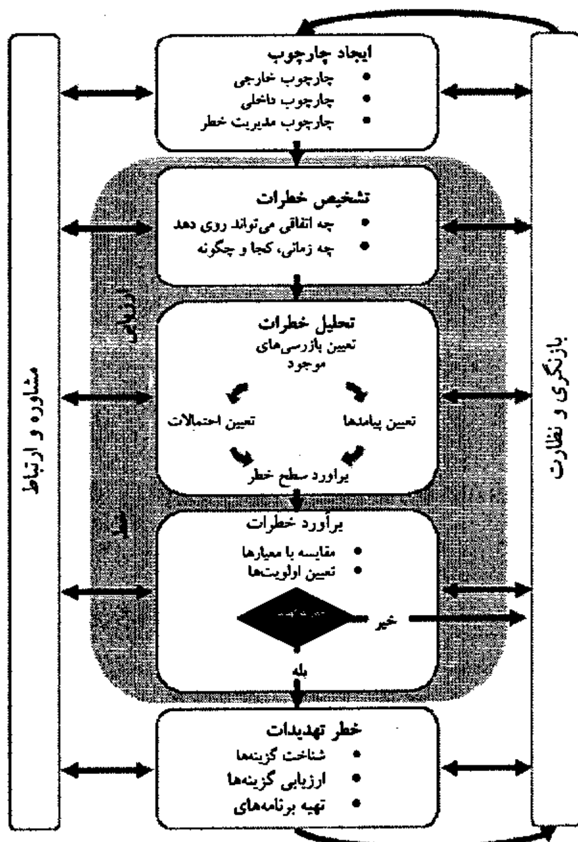
فرایند برآورد و ارزیابی مخاطرات در استرالیا دارای پنج مرحله شامل: *ایجاد زمینه، تشخیص مخاطرات، تحلیل مخاطرات، ارزیابی مخاطرات و تهدید مخاطرات* است.

این فرایند توسط دو مجموعه که در عرض این فرایند قرار دارند، جهت‌دهی و تعدیل می‌شود. یک مجموعه وظیفه رصد کردن و وارسی وضعیت را در مراحل پنج‌گانه را و نیز دریافت بازخورد از مرحله پنجم و تزریق داده‌ها به سیستم جهت آغاز مرحله جدید را به‌عهده

---

1. Emergency Ris Management 2. Emergency Management Astralia
3."Critical Infrastructure Emergency Risk Management and Assurance", **Handbook Emergency Management Australia, 2nd Edition, Nov. 2003.**

دارد. مجموعه دوم ارتباطات و مشاوره است. در این مجموعه نیز ارتباط با اعـضاء و همچنـین بخش‌های مختلف فرایند برقرار می‌گردد و ضمن دادن مشاوره به بخش‌هـای مختلـف فراینـد، دیدگاه‌های اعضاء را نیز به مجموعه‌های داخلی فرایند منتقل می‌نماید.



شکل ۹. دیاگرام مواجهه با مخاطرات ارائه شده توسط ERM

۳ـ۳. انگلستان

دولت انگلیس در حوزه CIIP دو نوع تهدید کلی را شناسایی و تدوین کرده است[1] که عبارتند از:

- حملات تروریستی به تأسیسات و تجهیزات؛
- حملات الکترونیکی به رایانه‌ها و سیستم‌های مخابراتی.

علاوه‌براین دولت در حوزه InfoSec نیز به شناسایی و تدوین شش نوع تهدید پرداخته است که عبارتند از:

- ویروس‌های رایانه‌ای؛
- هک کردن؛
- سیاست و عملکرد ناقص امنیتی؛
- حملات یا حوادث فیزیکی؛
- خطاهای سیستم در حوزه نرم‌افزار و سخت‌افزار؛
- خارج از رده بودن سیستم‌ها و نرم‌افزارها.

دولت بریتانیا در مواجهه با تهدیدات در حوزه فتا برآورد استراتژیک خود را با توجه به محورهای اساسی زیر تهیه می‌نماید:

- تحلیل بخش: این مرحله به تعریف و تبیین بخش‌های حیاتی می‌پردازد و مشخص می‌نماید که چه بخش‌ها و فضاهایی، حیاتی هستند.
- تحلیل وابستگی: این مرحله رابطه میان بخش‌های حیاتی با یکدیگر و فضاها و زیرفضاهای هریک از بخش‌های حیاتی با یکدیگر و نوع وابستگی‌های میان آنان را تعریف می‌کند.
- تحلیل خطی: در این مرحله روش‌های تحلیل خطی و چگونگی سنجش خطرهای مرتبط با CIIP و InfoSec مورد بررسی قرار می‌گیرد.
- ارزیابی تهدیدات: با توجه به روش و معیارهای سنجش خطر، تهدیدات موجود در

---

1. "Protecting our Information Systems", Central Sponser for Information Assurance, 2004.

حوزه فتا برآورد می‌گردد.

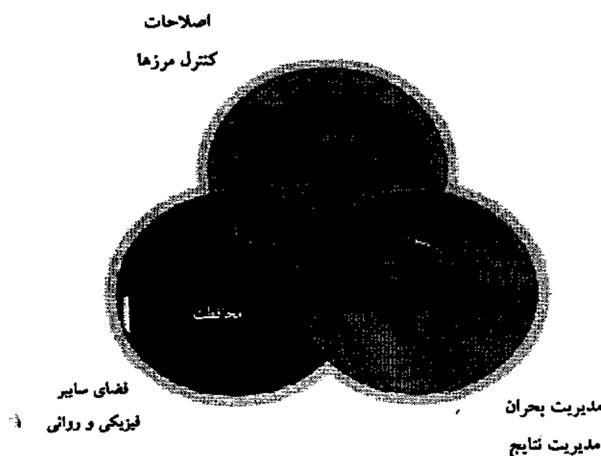
- ارزیابی آسیب‌پذیری‌ها: در این مرحله نیز با توجه به روش و معیارهای سنجش خطر، آسیب‌پذیری‌های موجود در زیرساخت‌ها، فضاها و زیرفضاهای حیاتی برآورد می‌شود.
- تحلیل سیستم: در این مرحله کلیه سیستم‌های مرتبط با زیرساخت‌های حیاتی و نقاط حیاتی و حساس آن مورد بررسی قرار می‌گیرد.
- ارزیابی لطمه:[1] در این مرحله اثر ضربه و نتایج آن مورد بررسی قرار می‌گیرد. دراین‌راستا و براساس روش انتخاب‌شده‌ای برای ارزیابی لطمه، انواع مختلف حمله و لطمات آن ازنظر ناحیه، زمان، دوام، شدت و روش مقابله با آن بررسی می‌گردد.

۳ـ۴. سنگاپور

بیشتر موارد مربوط به حفاظت از زیرساخت‌های حیاتی در سنگاپور نظیر ساختار و سازمان‌های دیگر همانند مدل آمریکا و استرالیاست؛ اما استراتژی این کشور در حوزه CIIP دارای جنبه‌های آموزشی مناسبی است.

استراتژی امنیتی سنگاپور در حوزه فتا یک استراتژی سه حلقه‌ای است که شامل: جلوگیری[2]، حفاظت و واکنش می‌شود. استراتژی جلوگیری به‌منظور شناسایی تهدیدات و مقابله با آن قبل از به‌فعلیت درآمدن متمرکز است. استراتژی حفاظت، برپایه ایمن‌سازی و محافظت از زیرساخت‌های حیاتی بنا شده و استراتژی واکنش نیز در برابر حادثه امنیتی و نحوه مقابله با آن طراحی گردیده است.[3]

1. Impact Assessment 2. Prevention
3. http://www.cisco.com.sg/service/index.html



شکل ۲. فضای Syber در سنگاپور

۳ـ۵. ایران

موضوعیت زیرساخت‌های حیاتی، اطلاعاتی و زیرفضاهای اطلاعاتی مربوط به سایر زیرساخت‌های حیاتی بستگی به میزان گستردگی، شبکه‌ای بودن، اهمیت آن در قدرت و منافع ملی و به‌دنبال آن امنیت ملی یک کشور دارد. در برخی از کشورها اصولاً CII موضوعیت ندارد؛ زیرا در این کشورها یا چنین زیرساخت‌هایی وجود ندارد یا بسیار ابتدایی است.

ازسوی‌دیگر اهمیت حفاظت از زیرساخت‌ها به اینترنتی یا اینترانتی بودن این زیرساخت‌ها بستگی دارد. چنانچه زیرساخت‌هایی در حوزه CII اینترنتی باشند، به‌تحقیق حفاظت از آن از اهمیت مضاعفی برخوردار خواهد بود؛ درحالی‌که این امر در اینترانتی بودن CII مانند گزینه قبلی، پیچیده و حساس نیست.

جمهوری اسلامی ایران در ده سال گذشته از رشد چشمگیری در حوزه فتا برخوردار بوده که تاکنون نیز ادامه یافته است و با توجه به برنامه‌های مدون و نهادهای ایجادشده و چشم‌انداز موجود، این رشد همچنان و با سرعت نسبتاً بالا ادامه خواهد یافت.

در این چارچوب نیز بسیاری از زیرساخت‌های کشور به‌صورت اجتناب‌ناپذیری به‌سمت بهره‌برداری هرچه بیشتر از تکنولوژی اطلاعات پیش خواهد رفت و همچنین زیرساخت‌های اطلاعاتی نیز توسعه پیدا خواهند کرد. در چنین شرایطی تمهیدات لازم به‌منظور حفاظت از چنین زیرساخت‌هایی اهمیت زیادی پیدا می‌کند. بدیهی است طراحی، سازمان، ساختار، فرایند، ابزار، نیروی انسانی ماهر و مدیریت در حوزه حفاظت از زیرساخت‌های حیاتی به اندازه خود زیرساخت‌ها مهم هستند. البته هنوز گستردگی، پیچیدگی، شبکه‌ای شدن و اینترنتی گردیدن زیرساخت‌های حیاتی جمهوری اسلامی در حد برخی کشورهای پیشرو نیست؛ لذا ضرورتی در به‌کارگیری سیستم‌ها، ساختارها، فرایندها و ابزارهای حفاظتی مشابه آنان وجود ندارد. بدیهی است چنین رویکردی نه‌تنها مؤثر و کارآمد نخواهد بود، بلکه ضمن برجای گذاشتن هزینه‌های گسترده باعث ایجاد مشکلات جانبی در کار نیز خواهد شد.

نکته مهم دیگر این است که اهمیت، جایگاه و ویژگی‌های زیرساخت‌های حیاتی اطلاعاتی و فضاها و زیرفضاهای اطلاعاتی با دیگر زیرساخت‌های غیرحیاتی، همان‌طورکه در بخش اول توضیح داده شد متفاوت است. بنابراین از جنبه‌های امنیتی جداسازی حفاظت از زیرساخت‌های حیاتی از زیرساخت‌های غیرحیاتی ضروری به‌نظر می‌آید.

با توجه به این نکات ایجاد یک شورای عالی امنیت زیرساخت‌های حیاتی در کشور که مأموریت سیاستگذاری و تعیین خط‌مشی‌ها و بررسی و تصویب طرح‌ها و پروژه‌های ملی امنیت زیرساخت‌های حیاتی را عهده‌دار شود، ضروری به‌نظر می‌رسد. همچنین شناسایی و تعیین زیرساخت‌های حیاتی باید در درون این شورا انجام پذیرد. بنابراین افزودن یا حذف مواردی از فهرست زیرساخت‌های حیاتی کشور در این شورا صورت خواهد گرفت.

نکته دوم اینکه ایجاد کانون تحلیل مخاطرات مربوط به زیرساخت‌های مطروحه نیز امری ضروری است. بدیهی است با توجه به طبقه‌بندی‌های حفاظتی در هریک از فضاها و زیرفضاهای مربوط به زیرساخت‌های حیاتی، ایجاد چنین کانون‌هایی در درون هریک از سازمان‌های متولی چنین فضایی امری ضروری و لازم است. این کانون‌ها مانند دیگر مراکز

تحلیل اطلاعات شایسته است که در فرایندی ازپیش تعریف‌شده شامل: تشخیص مخاطرات، تحلیل مخاطرات، برآورد ابعاد، سطوح، عمق و شدت مخاطرات به بررسی مخاطرات مربوط به فتا در حوزه و سازمان مربوطه بپردازد.

نکته سوم ایجاد مرکز فوریت‌های حوادث امنیتی در حوزه فتا آن‌هم به‌صورت متمرکز در هر حوزه و سازمان مربوطه امری ضروری و شایسته است. بدیهی است به تناسب حجم و اندازه حوزه فتا در فضا یا زیرفضاهای حیاتی اطلاعاتی، سازمان چنین مرکزی باید گسترده شود. این مرکز که در بسیاری از کشورهای دنیا به نام (CERT) [1] شناخته می‌شود، نسبت به حوادث امنیتی در بخش‌های بحرانی مسئولیت خواهد داشت و مأموریت دارد تا پس از وقوع حادثه بلافاصله نسبت به آن واکنش نشان داده، درخصوص خنثی‌سازی حادثه اقدام نماید.

در کنار حوزه‌ها و مراکز و طرح‌های اختصاصی مربوط به حفاظت از زیرساخت‌های حیاتی که به‌صورت منفصل و توسط سازمان‌های مربوطه انجام می‌شود، بسیاری از نیازمندی‌های مربوط به امنیت زیرساخت‌های حیاتی از حوزه‌های خصوصی و عمومی مربوطه در داخل و خارج از کشور قابل تأمین هستند؛ برای مثال دیگر نیازی نیست که برای آموزش کادرها و مأموران مرتبط با زیرساخت‌های حیاتی، آموزشکده و یا مرکز جداگانه‌ای تأسیس کرد و می‌توان از مراکز موجود در کشور براساس آنچه تدارک دیده‌شده استفاده نمود.

---

1. Computer Emergency Response Team

کتابنامه

الف) منابع فارسی

۱. آدامز، جیمز. «دفاع مجازی». ترجمه حسین سلیمی. **فصلنامه سیاست خارجی**. سال پانزدهم، شماره ۳، پاییز ۱۳۸۰.

۲. صدوقی، مرادعلی. **تکنولوژی اطلاعاتی و حاکمیت ملی**. تهران: وزارت امورخارجه، مرکز چاپ و انتشارات، ۱۳۸۰.

ب) منابع انگلیسی

3. "Critical Infrastructure Emergency Risk Management and Assurance". **Handbook Emergency Management Australia**. 2nd Ed. Nov. 2003.
4. "Information Dominance Edges toward New Conflict Frontier," **Signal**, No. 48, Aug. 1994.
5. "Xybernaut Plans Wearable PC", **Reuters, special to CNET News**. May 15, 1998.
6. "Xybernaut plans Wearable PC". **Reuters,** Special to CNET News. May 15, 1998.
7. Arquilla, John; Ronfeldt, David. "Cyberwar is Coming!" **Comparative Strategy**. No. 2, Apr-June 1993.
8. Arquilla, John; Ronfeldt, David. "Cyberwar is Coming!" **Comparative Strategy**. No. 12, Apr-June 1993.
9. Arquilla, John; Ronfeldt, David. "Cyberwar Is Coming". **Comparative Strategy,** Vol. 12, 1993.
10. Art, Robert J. **The Four Functions of Force**. New York: Harper Collins, 1996.
11. Barnett, Roger W. "Information Operations, Deterrence and the Use of Force", **Naval War College Review**. Vol. 51, No. 2, Spring 1998.
12. Bartov, Omer. **Hitler's Army**. Oxford: Oxford University Press, 1992.
13. Berkowitz, Bruce D. "Warfare in the Information Age". **Issues in Science and**

Technology. Fall 1995.

14. Bishop, Matt; Goldman, Emily O. "The Strategy and Tactics of Information Warfare". **Contemporary Security Policy.** Vol. 24, No. 1, Apr. 2003.
15. Boney, David G. "The Plague: An Army of Software Agents for Information Warfare", **paper for CS 229, George Washington University**. Dec. 11, 1997.
16. Boyd, John R. **Briefing slides, subject: A Discourse on Winning and Losing.** Maxwell AFB, Alabam, Aug. 1987.
17. Builder, Carl H. **The Icarus Syndrome: The Role of Air Power Theory in the Evolution and State of the U.S. Air Force**, New Brunswick, N.J.: Transaction Publishers, 1994.
18. Clausewitz, Carl Von. **On War**, Michael Howard and Peter Paret, eds and trans. Princeton; Guildford: Princeton University Press, 1976.
19. Cohen, Alex. "Net Politics: A Mover, but Not a Shaker", ***Wired News***. Apr. 8, 1998.
20. Demchak, Chris C. "Wars of Disruption: International Competition and Information Technology-Driven Military Organizations". **Contemporary Security Policy**. Vol. 24, No. 1, Apr. 2003.
21. Demchak, Chris C. "Watersheds in Perception and Knowledge: Twenty Years of Military Technology". **Draft Manuscript**. June 1999.
22. Denning, Dorothy E. **Information Warfare and Security**. New York, N.Y.: ACM Press; Harlow: Addison-wesley, 1999.
23. Denning, Dorothy E; Denning, peter J. "Data Security". **ACM Computing Surveys (CSUR)**. Vol. 11, No. 3, Sep. 1979.
24. Denning, Peter J. "The Internet after Thirty Years," in **Internet Besieged: Countering Cyberspace Scofflaws**. Dorothy E. Denning and Peter J. Denning, eds., Addison-Wesley, 1997.
25. Der Derian, James "Cyber-deterrent". **Wired News,** Vol. 2, No. 9, 2001.
26. Dewar, Micheal. **The Art of Deception in Warfare**. Newton Abbot: David & Charles, 1989.
27. Dunnigan, James F. **How to Make war: A Comprehensive Guide to Modern Warfare in twenty-First Century.** 4th ed. New York: HarperCollins Publishers, 2003.
28. Elliott, Christopher. "Everything Wired Must Converge", **Journal of Business Strategy**. Dec. 31, 1997.
29. Engelbrecht, Joseph A. **"War Termination: Why Does a State Decide to Stop Fighting?"**, PhD diss., Columbia University, 1992.
30. Folkers, Richard. "Xanadu 2.0," **U.S. News & World Report**. Dec. 1, 1997.
31. Gellman, Barton. "The Cyber-Terror Threat". **Washington Post National Weekly Edition**. 1-4 July 2002.
32. George, Alexander L. "Coercive Diplomacy: Definition and Characteristics", **in The Limits of Coercive Diplomacy**. Alexander L. George and William E. Simons, ed. Boulder: Westview Press, 1994.

33. Goldman, Emily O. "Security in the Information Technology Age". **Contemporary Security Policy.** Vol. 24, No. 1, April 2003.
34. Goldman, Emily O.; Eliason, Leslie. **Diffusion of Military Technology and Ideas.** Stanford, CA: Stanford University Press, 2003.
35. Hammond, Grant T. "Paradoxes of War," **JFQ: Joint Forces Quarterly**, Spring 1994.
36. Handel, Michael I. **Masters of War**. London: Frank Cass, 2001.
37. Harknett, Richard J. "Integrated Security, A Strategic Response to Anonymity and the Problem of the Few". **Contemporary Security Policy**. Vol. 24, No. 1, Apr. 2003.
38. Herman, Debra S. "Apractical Guide to Security Engineering and Information Assurance", **CRC press,** 2008.
39. Honc, K.; Eloff, J.H.P. "Information Security Policy: What do International Security Standard Say?". **Computer and Security.** Vol. 21, No. 5.
40. Howard, Michael. **War in Eurppean History**. Oxford: Oxford Univer-sity Press, 1976
41. Hurst, Gerald R. "Taking down Telecommunications", Thesis, School of Advanced Airpower Studies, Air University, Maxwell Air Force Base, Ala, 28 May 1993.
42. Jung, C.G. **The Undiscovered Self,** New York: The New American Library, Mentor Book, 1958.
43. Kahn, David. **The Codebreakers.** New York: Macmillan, 1967.
44. Kohn, George C. **Dictionary of Wars,** New York: Facts On File Publications, 1986.
45. Krepinevich, Andrew. "Cavalry to Computer: the Pattern of Military Revolutions", **The National Meres.** No. 37, Fall 1994
46. Lee, Dustin, et al. "Detecting and Defending Against Web-Server Fingerprinting", **18th Annual Computer Security Applications Conference.** 10-14 Dec.2007.
47. Lenhart, Jennifer. "Keeping an Electronic Eye on the Kids," **Washington Post.** May 29, 1998.
48. Libicki, Martin C. **What is Information Warfare?.** Washington, D.C.: Center for advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University, 1995.
49. libicki, Martin. "The Emerging Primacy of Information", ***Orbis***. Vol. 40, No. 2, Spring 1996.
50. Mader, Chris. **Information Systems: Technology, Economics, Applications.** Chicago: Science Research Associates, Inc., 1974.
51. Mahnken, Thomas G. "War in the Information Age". **Join: Force Quarterly**. Winter 1995-96.
52. Metz, Steven; Kievit, James. **Strategy and the Revolution in Military Affairs: From Theory to Policy**. Carlisle Barracks, Pa: Strategic Studies

Institute, U.S. Army War College, 1995.

53. Molander, Roger C.; Riddle, Andrew S. and Wilson, Peter A. **Strategic Information Warfare: A New Face of War**. Santa Monica, Calif: RAND: 1996.
54. Nash, Jim. "Wiring the Jet Set", **Wired News**. Oct. 1997.
55. Negroponte, Nicholas. "The Third Sall Be First", ***Wired News***. Vol. 6, No. 1, Jan. 1998.
56. Nye, Joseph S.; Owens, Jr.; Owens, William A. "America's Information Edge", **Foreign Affairs**. Vol. 75, No. 2, March-Apr. 1996.
57. Nye, Jr., Joseph S.; Owens, William A. "America's Information Edge". **Foreign Affairs**. Vol. 75, No. 2, March-Apr. 1996.
58. Parker, Donn B. "Automated Crime," in **Cybercrime**, International Conference Course Book, Oceana Publications, Washington, DC, Oct. 30-31, 1997; New York, Nov. 17-18, 1997.
59. Petersen, John. "Information Warfare: The Future", in **Cyberwar: Security, Strategy and Conflict in the Information Age**. Alan D. Campen, Douglas H. Dearth, and Thomas Gooden, eds., AFCEA International Press, Fairfax, VA, 1996.
60. Post, Jonathan V. "Cybernetic War". **Omni**. May 1979.
61. Reid, B. "Reflections on some Widespread Computer Break-Ins". **Gommunications of the ACM**. Vol. 30, No. 2, Feb. 1987.
62. Rosenzweig, Paul; Kochems, Alane; Schwartz, Air. "Biometric Technologies: Security, Legal and Policy Implications", **Legal Memorandum.** No. 12, 2004.
63. Rue, Loyal. By the Grace of Guile: The Role of Deception in Natural History and Human Affairs. New York: Oxford University Press, 1994.
64. Runes, Dagobert D. ed. **Dictionary of Philosophy**, Totowa, N.J.: Littlefield, Adams & Co., 1962.
65. Schiesel, Seth. "Taking Aim at an Enemy's Chips". **New York Times**. 20 Feb. 2003.
66. Schwartau, Winn. **Information Warfare: Chaos on the Electronic Superhighway**. New York: Thunder's Mouth, 1994.
67. Schwartau, Winn. **Information Warfare: Chaos on the Electronic Superhighway**. New York: Thunder's Mouth, 1994.
68. Shamon, C. E. "Communication Theory of Secrecy Systems". **Bell System Technical**. Vol. 28, No. 4.
69. Shanker, Thom; Schmitt, Eric. "Firing Leaflets and Electrons, US. Wages Information War". **New York Times,** 24 Feb. 2003.
70. Spitzner, L. **Honeypots: Tracking Hackers**. Boston, MA: Addison Wesley Professional, 2002.
71. Stein, George J. "Information War-Net War-Cyber war", in **Battlefield of the Future: 21st Century Warfare Issues.** B.R. Schneider and L.E. Grinter, eds. Maxwell AFB, Ala: Air University Press, 1995.

72. Stoll, Clifford. "Stalking the Wily Hacker", **Communications of the AGM**. Vol. 31, No. 5, May. 1988.
73. Sullivan, Jr., L. **Meeting the Challenges of Regional Security**. Carlisle, PA: US Army War College Strategic Studies Institute, 1994.
74. Szafranski, Richard. "A Theory of Information Warfare: Preparing for 2020" **Airpower journal**. Vol. 9, No. 1, Spring 1995.
75. Szafranski, Richard. "Toward a Theory of Neocortical Warfare: Pursuing the Acme of Skill," **Military Review**. Nov. 1994.
76. Szafranski, Richard. "When Waves Collide: Conflict in the Next Century," **JFQ: Joint Force Quarterly**. Winter 1994-95.
77. Thomas, Timothy L. "Deterring Information Warfare: A New Strategic Challenge". **Parameters.** Winter 1996-97.
78. Toffler, Alvin. **The Third Wave**. London: Collins, 1980.
79. Toffler, Alvin; Toffler, Heidi. "Foreword: The New Intangibles",in **In Athena's Camp: Preparing for Conflict in the Information Age**. John Arquilla and David Ronfeldt, eds. Santa Monica, CA: RAND, 1997.
80. Toffler, Alvin; Toffler, Heidi. **War and AntiWar: Survival at the Dawn of the 21st Century**. Boston: Little, Brown, 1993.
81. Tzu, Sun. **The Art of War**. trans. Samuel B. Griffith, New York: Oxford University Press, 1977.
82. Weiss, Rick. "Neurology: Computer Chips for the Brain", **Washington Post**. Oct. 27, 1997.
83. Wheatley, G.F.; Hayes, R.E. **Information Warfare and Deterrence**. Washington DC: National Defense University Press, 1996.

فهرست محصولات مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی تهران

کتاب‌های مرجع

عناوین	سال انتشار
راهنمای مراکز مطالعاتی جهان ـ جلد سوم (مراکز مطالعات اروپا، آمریکا، آفریقا)	۸۶
راهنمای سازمان‌های غیردولتی (چاپ ۲ با اصلاحات و اضافات)	۸۶
راهنمای مراکز مطالعاتی جهان ـ جلد دوم (مراکز منطقه‌ای)	۸۴
جهانی شدن سیاست (۱) و(۲)	۸۴
دانشنامه نخبگان (۱)	۸۳
راهنمای منطقه خزر	۸۳
راهنمای منطقه و کشورهای حوزه خلیج‌فارس	۸۳
راهنمای مراکز مطالعاتی جهان جلد اول (مراکز مطالعات استراتژیک، بین‌المللی، سیاست و روابط خارجی و علوم سیاسی)	۸۲

کتاب‌های برآورد استراتژیک

عناوین	سال انتشار
آشنایی با کشورهای اسلامی (جمهوری اسلامی ایران)	۸۵
برآورد استراتژیک ترکیه	۸۵
آشنایی با کشورهای اسلامی (پاکستان)	۸۵
برآورد استرتژیک عربستان	۸۴
آشنایی با کشورهای اسلامی (تــرکیــه)	۸۴
آشنایی با کشورهای اسلامی (مالزی)	۸۴
آشنایی با کشورهای اسلامی عربی (مصر)	۸۴
برآورد استراتژیک آمریکا (سرزمینی ـ سیاسی)	۸۲
براورد استراتژیک آذربایجان (سرزمینی، سیاسی، فرهنگی)	۸۲
برآورد استراتژیک پاکستان	۸۲
برآورد استراتژیک ژاپن	۸۲
برآورد استراتژیک مصر	۸۱

کتاب‌های تخصصی

عناوین کتاب	سال انتشار
همه چیز درباره نظرسنجی	۸۶
ایجاد شبکه‌هایی از مسلمانان میانه‌رو	۸۶
فرهنگ استراتژیک	۸۶
تروریسم‌شناسی	۸۶
مرزهای ایران	۸۶
اصلاحات سیاسی در عربستان سعودی (تاثیر بحران عراق بر تحولات سیاسی عربستان)	۸۶
مقدمه‌ای بر سیاست و حکومت در آفریقا	۸۶
جنگ (رسانه‌ها و تبلیغات)	۸۶
پرونده هسته‌ای ایران ۳ (روندها و نظرها)	۸۶
جنگ نرم ۲ (چاپ دوم) ویژه جنگ رسانه‌ای	۸۶
جنگ نرم ۱ (چاپ دوم) ویژه جنگ رایانه‌ای	۸۶
امنیت بین‌الملل ۱ (چاپ ۲) (فرصت‌ها، تهدیدات و چالش‌های فراروی امنیت ملی جمهوری اسلامی ایران)	۸۶
پرونده هسته‌ای ایران (۱) چاپ ۲ (روندها و نظرها)	۸۶
رویکردها و طرح‌های آمریکایی درباره ایران	۸۶
پان‌ترکیسم و پان آذریسم (مبانی اهداف و نتایج)	۸۶
تجدید حیات امپراتوری (رد پای غرب و مسیر مخاطره‌آمیز آمریکا درخاورمیانه)	۸۵
ساختار دولت رژیم صهیونیستی (دوجلدی)	۸۵
امنیت در قفقاز جنوبی	۸۴
پرونده هسته‌ای ایران (۲) (روندها و نظریه‌ها)	۸۴
هیدروپولیتیک رودهای مرزی	۸۴
افسانهٔ انقلاب‌های رنگی	۸۴
دیباچه‌ای بر قانون امنیت ملی: مقدمه‌ای بر طرح‌ریزی دکترین امنیت ملی (۳)	۸۴
سیاست و توسعه در جهان سوم	۸۴
روابط ایران و انگلستان (جلد اول)	۸۴
آلمان: منافع جمهوری اسلامی ایران	۸۴
سیاست خارجی روسیه	۸۴
چالش‌های هویت در آمریکا	۸۴
مصائب امپراتوری (امپریالیسم نظامی آمریکا در قرن ۲۱)	۸۴

عناوین	سال انتشار
حقوق و امنیت در فضای سایبر	۸۴
امنیت بین‌الملل ۳ (فرصت‌ها، تهدیدات و چالش‌های فراروی امنیت ملی جمهوری اسلامی ایران)	۸۴
امنیت بین‌الملل ۲ (فرصت‌ها، تهدیدات و چالش‌های فراروی امنیت ملی جمهوری اسلامی ایران)	۸۴
تنها ابرقدرت (هژمونی آمریکا در قرن ۲۱)	۸۳
جنگ نرم ۱ (ویژه جنگ رایانه‌ای)	۸۳
جنگ نرم ۲ (ویژه جنگ رسانه‌ای)	۸۳
سازمان‌های امنیتی در کشورهای مدل (انگلستان ـ فرانسه، ایتالیا و کانادا)	۸۳
دموکراسی، قانون، امنیت (بررسی سرویس‌های اطلاعاتی در غرب)	۸۳
پرونده هسته‌ای ایران (روندها و نظرها)	۸۳
سنجش قدرت ملی در عصر فراصنعتی	۸۳
طرح خاورمیانه بزرگتر (القاعده و قاعده در راهبرد امنیت ملی آمریکا)	۸۳
آشنایی با معاهده گسترش سلاح هسته‌ای و پروتکل	۸۳
روزهای سرنوشت‌ساز آلمان (تاریخ معاصر آلمان ۱۹۸۹ تا ۱۹۱۴)	۸۳
تظاهرات ضد جنگ	۸۳
دعاوی ایران (بررسی کمک و حمایت‌های غرب به‌ویژه آمریکا از صدام حسین در جنگ تحمیلی)	۸۳
نظریه‌های امنیت ۱ (مقدمه‌ای بر طرح‌ریزی دکترین امنیت ملی)	۸۳
حاکمیت قدرت	۸۳
رژیم‌های بین‌المللی	۸۳
مناقشه قره‌باغ آرمان‌ها و واقعیت‌ها	۸۳
روابط ایران و آمریکا (بررسی دیدگاه نخبگان آمریکایی)	۸۲
گسل‌های منازعه	۸۲
سیاست خارجی آمریکا در آسیا	۸۲
مسائل ایران و عراق	۸۲
استراتژی در جهان معاصر (مقدمه‌ای بر مطالعات استراتژیک)	۸۲

عناوین	سال انتشار
استراتژی امنیت ملی آمریکا در قرن ۲۱	۸۲
عملیات اژاکس (بررسی اسناد CIA درباره کودتای ۲۸ مرداد)	۸۲
جنگ آمریکا و عراق	۸۱
دیپلماسی آمریکا در قرن ۲۱	۸۱
اصلاحات در چین و شوروی	۸۰

کتاب‌های منطقه‌ای

عناوین	سال انتشار
کتاب خاورمیانه (۳) (چاپ ۲) (ویژه بررسی مسائل داخلی رژیم صهیونیستی)	۸۶
کتاب خاورمیانه (۲) (چاپ ۲) (ویژه حضور اسرائیل در مناطق هم‌جوار ایران)	۸۶
کتاب خاورمیانه ۱ (چاپ ۲) (ویژه مسائل و چالش‌های خاورمیانه)	۸۶
کتاب اروپا (۷) (ویژه رویکردهای امنیتی اتحادیه اروپا)	۸۵
خاورمیانه (۵) (ویژه اصلاحات در خاورمیانه)	۸۵
کتاب امریکا (۷) (ویژه دکترین امنیت ملی آمریکا)	۸۵
کشورهای مستقل مشترک‌المنافع ۲ (ویژه ملاحظات سیاست خارجی و امنیتی روسیه)	۸۴
کتاب خاورمیانه (۴) (ویژه خلیج‌فارس)	۸۴
کتاب خاورمیانه ۳ (ویژه بررسی مسائل داخلی رژیم صهیونیستی)	۸۴
کتاب خاورمیانه ۲ (ویژه حضور اسرائیل در مناطق هم‌جوار ایران)	۸۴
کتاب آسیا ۳ (ویژه افغانستان پس از طالبان)	۸۴
کتاب امریکا ۷ (ویژه دکترین امنیت ملی آمریکا)	۸۴
کتاب امریکا ۶ (ویژه دیپلماسی عمومی آمریکا)	۸۴
کتاب اروپا ۶ (ویژه ناتو)	۸۴
کتاب اروپا ۵ (ویژه روابط آمریکا و انگلیس)	۸۴
کتاب امریکا ۴ (ویژه نومحافظه‌کاران)	۸۳

عناوین	سال انتشار
کتاب امریکا ۵ (ویژه نظام انتخاباتی آمریکا)	۸۳
کتاب اروپا ۳ (ویژه روابط ایران و اتحادیه اروپا)	۸۳
کتاب اروپا ۴ (ویژه روابط اروپا و آمریکا)	۸۳
کتاب آسیا ۲ (ویژه بحران‌های آسیا)	۸۳
کشورهای مستقل مشترک‌المنافع ۱ (ویژه مسائل امنیتی CIS)	۸۳
کتاب خاورمیانه ۱ (ویژه مسائل و چالش‌های خاورمیانه)	۸۳
کتاب اسیا ۱ (ویژه مسائل امنیتی شرق آسیا)	۸۲
کتاب افریقا (ویژه منازعات مسلحانه)	۸۲
کتاب امریکا ۱ (ویژه دکترین امنیت ملی بوش در خاورمیانه)	۸۲
کتاب امریکا ۲ (ویژه سیاست‌های امنیتی ایالات‌متحده در عراق)	۸۲
کتاب امریکا ۳ (ویژه روابط آمریکا ـ اسرائیل)	۸۲
کتاب اروپا ۱ (اتحادیه اروپا)	۸۲
کتاب اروپا ۲ (ویژه روابط ایران و اتحادیه اروپا)	۸۲

گزیده پژوهش‌های جهان

عناوین	سال انتشار
گزیده پژوهش‌های جهان ۵ (جهانی شدن و ماهیت جنگ ـ پشت پرده: روابط اسرائیل و پاکستان ـ تحول دکترین نظامی روسیه ـ اتحادیه اروپا و بحران در خاورمیانه)	۸۲
گزیده پژوهش‌های جهان ۴ (مبارزه با تروریزم ـ بازسازی عراق ـ منازعات هسته‌ای قرن ۲۱ ـ امنیت ملی روسیه ـ امنیت پس از ۱۱ سپتامبر و ....)	۸۲
گزیده پژوهش‌های جهان ۳ (تحول مفاهیم امنیت ملی در قرن ۲۱ ـ پارادوکس قدرت آمریکا ـ چارچوبی برای تدوین استراتژی ـ مشارکت فرار ـ آینده امنیت منطقه فرا خزر)	۸۱
گزیده پژوهش‌های جهان ۲ (ساختار امنیتی آینده در خاورمیانه ـ سلاح‌های هسته‌ای در قرن ۲۱ ـ پیامدهای امنیتی خیزش چین در آسیا ـ سیاست در ۵۰ سال آینده ـ برآورد استراتژیک اوراسیای مرکزی)	۸۱
گزیده پژوهش‌های جهان ۱ (سنجش قدرت ملی در عصر فراصنعتی ـ دریای خزر ـ انقلاب اطلاعاتی در ابعاد جهانی ـ خشونت سیاسی و ثبات)	۸۱

گزیده تحولات

عناوین کتاب	سال انتشار
گزیده تحولات ۲۵ تا ۳۷	۸۳-۸۴
گزیده تحولات ۱۳ تا ۲۴	۸۲-۸۳
گزیده تحولات ۱ تا ۱۲	۸۰-۸۱

کتاب‌های ایران‌ریویو

عناوین کتاب	سال انتشار
ایران‌ریویو ۳	۸۳
ایران‌ریویو ۲	۸۲
ایران‌ریویو ۱	۸۲

پژوهش و تحقیق

عناوین	سال انتشار
مسلمانان در انگلیس	۸۶
انگلستان و اتحادیه اروپا (تقابل یا همکاری)	۸۶
نگاهی به لابی ارامنه در ایالات متحده	۸۶
نگاهی به احزاب عمده و مؤثر در سیستم حکومتی انگلستان	۸۶
براندازی نرم (مطالعه موردی لتونی)	۸۶
براندازی نرم (جمهوری شیلی)	۸۶
براندازی نرم (جمهوری گرجستان)	۸۶
برآورد استراتژیک انگلستان (سرزمینی ـ سیاسی)	۸۵
بررسی پروژه احداث جزایر مصنوعی امارات عربی متحده در خلیج‌فارس	۸۵
گزارش بیکر ـ همیلتون: نگاهی عمیق به وضعیت آمریکا در عراق	۸۵
بررسی اختلافات سرزمینی در دیوان بین‌المللی دادگستری: مطالعه موردی ادعای امارات بر جزایر سه گانه	۸۵

عناوین	سال انتشار
جورج سورس و انقلاب‌های مخملین	۸۵
تصاویر ماهواره‌ای گوگل و پیامدهای آن	۸۵
مجمع پارلمانی ناتو و دیدگاه‌های ایران پیرامون جمهوری اسلامی ایران	۸۵
مدیریت تصاویر ذهنی در ادبیات کاخ سفید در مورد جمهوری اسلامی ایران	۸۴
مراکز فکری تاثیرگذار در سیاست خارجی و امنیتی انگلیس	۸۴
اسیب‌شناسی دیپلماسی و سیاست خارجی جمهوری اسلامی ایران	۸۴
نگاهی به پدیده دولت‌های ورشکسته	۸۴
اینترنت در ایران (بررسی کارکردهای مثبت و منفی اینترنت و وبلاگ در ایران)	۸۴
نگاهی به پژوهش‌های مؤسسات تحقیقاتی (سیاست و روابط خارجی، مسائل منطقه‌ای، امنیتی و استراتژیک)	۸۴
تروریسم در پرتو تکوین نظام حقوقی بین‌المللی: خاستگاه مبهم سیاسی، استلزامات حقوقی کیفری	۸۴
بررسی وضعیت مرز ایران و افغانستان	۸۳
نظر مشورتی دیوان بین‌المللی دادگستری در تضیه آثار حقوقی ساخت دیوار در سرزمین اشغالی فلسطین	۸۳
قانون و امنیت در کشورهای مدل	۸۳
نقش شیعیان در فرایند دولت‌سازی عراق نوین و تأثیر آن بر امنیت ملی جمهوری اسلامی ایران	۸۳

بولتن ویژه

عناوین	سال انتشار
جوامع شرقی اسرائیل	۸۶
تصوف در آسیای مرکزی	۸۶
سلفی‌گری در جهان اسلام	۸۶
لابی و لابی‌گر در ایالات متحده	۸۶
نگاهی به گروه‌های مسلح در عراق	۸۶
تحریم‌ها علیه ایران: مسائل اساسی	۸۶
بازدارندگی (کلید حل مسئله هسته‌ای ایران)	۸۶

عناوین	سال انتشار
ادبیات کاخ سفید ۱۰ (بررسی دیدگاه‌های موجود در آمریکا درخصوص ایران آبان ۸۶)	۸۶
ادبیات کاخ سفید ۹ (بررسی دیدگاه‌های موجود در آمریکا درخصوص ایران مرداد ۸۶)	۸۶
ادبیات کاخ سفید ۸ (بررسی دیدگاه‌های موجود در آمریکا در خصوص ایران تیر ۸۶)	۸۶
ادبیات کاخ سفید ۷ (بررسی دیدگاه‌های موجود در آمریکا در خصوص ایران دی و بهمن ۱۳۸۴)	۸۵
حضور نومحافظه کاران در بریتانیا	۸۵
ترکیه: مسیری برای ترانزیت انرژی	۸۵
منابع آمریکایی حامی اسراییل	۸۵
مجاهدین خلق: چپ‌های دیوصفت	۸۵
حق بازگشت (از قطعنامه۱۹۴تا قراردادژنو)	۸۵
ایران راه‌های خروج از بن‌بست هسته‌ای	۸۵
تحلیل نقش جنگ‌سالاران به‌ویژه اسماعیل‌خان در افغانستان و ارتباط آن با ایران و آمریکا	۸۴
بررسی تحلیلی و تاریخی سیاست بریتانیا در قبال اسرائیل	۸۴
دیپلماسی عمومی بریتانیا در عصر دودستگی‌ها	۸۴
انرژی و نانوتکنولوژی: استراتژی برای آینده	۸۴
سازمان همکاری شانگهای شکل‌گیری و دورنمای توسعه	۸۴
ادبیات کاخ سفید (۶) (بررسی دیدگاه‌های موجود در خصوص ایران خرداد و تیر ۸۴)	۸۴
راه‌حل‌های واقعی برای حل بحران هسته‌ای ایران	۸۴
بازی بزرگ نامعلوم؛ روسیه و مسئله هسته‌ای ایران	۸۴
روابط پاکستان ـ ایالات‌متحده: گام‌های بعدی	۸۴
گفت‌وگوی استراتژیک آمریکا و هندوستان	۸۴
ثبات سیاسی در کشورهای عربی: معضلات اقتصادی	۸۴
جابه‌جایی شن‌ها: پایان همکاری ایالات‌متحدهٔ آمریکا ـ عربستان سعودی	۸۴
روابط ایران ـ ایالات‌متحده: تحلیلی بر سیاست‌ها، قوانین و مقررات	۸۴

عناوین	سال انتشار
روابط ایران ـ ایالات‌متحده از دید شورای روابط سیاست خارجی	۸۴
روابط بین‌الملل در اسیای مرکزی ـ شرقی؛ چالش‌های ژئوپلیتیک و چشم‌انداز همکاری‌های سیاسی	۸۴
فهم تصوف و نقش بالقوه آن در سیاست خارجی آمریکا	۸۴
ایالات متحده، ایران و روابط فراآتلانتیک؛ به سوی بحران؟	۸۴
محافظت از تسلیحات و مواد هسته‌ای	۸۳
دروازه ترکیه (ترانزیت انرژی و مسائل امنیتی)	۸۳
پیامدهای جهانی دستیابی ایران به سلاح‌های هسته‌ای	۸۳
اسرائیل و موشک ضد موشک آرو	۸۳
عملگرایی در اوضاع سیاسی ایران	۸۳
روابط هسته‌ای ایران و روسیه و گزینه‌های سیاسی آمریکا	۸۳
بازگشت یهودستیزی	۸۳
نگاهی تحلیلی به روابط هند و اسرائیل	۸۳
بمب اتمی ایران: دیدگاه‌های ایران و آمریکا	۸۳
تحولات سیاسی و امنیتی اسرائیل	۸۳
پایان دادن به شرارت (چگونه می‌توان در جنگ علیه ترور پیروز شد)	۸۳
نگاهی تحلیلی به اعطای وضعیت تحت‌الحفظ از سوی آمریکا به اعضای گروهک رجوی	۸۳
خلاصه اجرایی گزارش کمیسیون ۱۱ سپتامبر	۸۳
نگاهی تحلیلی به مهم‌ترین مصوبات کنگره آمریکا علیه جمهوری اسلامی ایران	۸۳
شکل‌گیری ولکان‌ها (تاریخچه کابینه جنگ بوش)	۸۳
گفتگوهایی درباره عراق	۸۳
پایان دادن به شرارت	۸۳
افکار عمومی آمریکا و سیاست خارجی در سال ۲۰۰۴	۸۳
ادبیات کاخ سفید ۵ (بررسی اظهارات دولتمردان ایالات متحده در مرداد و شهریور ۱۳۸۳)	۸۳

عناوین	سال انتشار
ادبیات کاخ سفید ۴ (بررسی اظهارات دولتمردان ایالات متحده در خرداد و تیر ۱۳۸۳)	۸۳
ادبیات کاخ سفید ۳ (بررسی اظهارات دولتمردان ایالات متحده در ۶ ماهه دوم سال ۸۲)	۸۳
ادبیات کاخ سفید ۲ (بررسی اظهارات دولتمردان ایالات متحده در فروردین و اردیبهشت ۱۳۸۳)	۸۳
ادبیات کاخ سفید ۱ (بررسی اظهارات دولتمردان ایالات متحده در شش ماهه نخست سال ۱۳۸۲)	۸۲
سیاست خارجی دولت جدید ایالات متحده (نحوه تأثیر نتایج انتخابات ریاست جمهوری ایالات متحده بر ژئوپلیتیک و ادراکات جهانی)	۸۳
اروپا و طرح خاورمیانه بزرگ‌تر آمریکا: مسائلی اساسی برای گفت‌وگو	۸۳
پشت صحنه یک رابطه جنجال‌آمیز: ایالات متحده و ایران	۸۳
دیدگاه‌های مردم عراق درباره اشغال این کشور و آینده آن	۸۳
راهنمای مراکز ایران‌شناسی	۸۲
گزینه‌های پیش‌رو: سیاست ایالات متحده در برابر برنامه هسته‌ای ایران	۸۲
کنترل سلاح‌های کشتار جمعی (یافته‌های ۱۱ پروژه پژوهشی)	۸۲
افکار عمومی اسرائیل در خصوص امنیت ملی (۲۰۰۳)	۸۲
نگاهی به تحولات جهان (شش ماهه نخست سال ۱۳۸۲)	۸۲

